Facultad de Formación del Profesorado y Educación

Departamento de Didáctica y Teoría de la Educación

Doctorado en Educación

Hábitos seguros y responsables en el uso de las TIC: Diseño y evaluación de un plan de intervención para su desarrollo en la adquisición de las competencias digitales del alumnado de Educación Secundaria Obligatoria

Autor: Sergio Montero García

Director: Melchor Gómez García

Tesis doctoral presentada por:

Sergio Montero García

Con el título

Hábitos seguros y responsables en el uso de las TIC: Diseño y evaluación de un plan de intervención para su desarrollo en la adquisición de las competencias digitales del alumnado de Educación Secundaria Obligatoria

Facultad de Formación de Profesorado y Educación

Departamento de Didáctica y Teoría de la Educación

Dirigida por Melchor Gómez García

Madrid, septiembre de 2017

ABSTRACT TESIS DOCTORAL

Título: Hábitos seguros y responsables en el uso de las TIC: Diseño y evaluación de un plan de intervención para su desarrollo en la adquisición de las competencias digitales del alumnado de Educación Secundaria Obligatoria.

Palabras clave: TIC, riesgos, educación, seguridad, hábitos seguros.

Los niños y jóvenes, nativos digitales, han nacido inmersos en la *Sociedad de la Información,* en la que participan activamente aprovechando al máximo sus posibilidades de comunicación y socialización. De forma paralela al avance de las tecnologías de la información y la comunicación, aparecen escenarios que pueden generar situaciones de riesgo para los menores, los cuales han sido capaces de adquirir ciertas habilidades tecnológicas, sin embargo, no han sido capaces de desarrollar del mismo modo hábitos seguros y responsables en el uso de las TIC. Los riesgos derivados del uso de las TIC supone para los niños y adolescentes la exposición a daños potenciales para su seguridad, bienestar y desarrollo.

La presente investigación pretende favorecer la adquisición de hábitos seguros y responsables en el desarrollo de las competencias digitales de los jóvenes de 2º de la ESO, que permitan contrarrestar los riesgos y consecuencias nocivas que derivan del uso de las TIC. Para ello, se ha creado un plan de intervención que utiliza un diseño cuasi-experimental con grupos de control no equivalente. La muestra total es de 107 alumnos de segundo curso de Educación Secundaria Obligatoria con edades comprendidas entre los 12 y los 16 años. El grupo experimental, que recibió el tratamiento consistente en 2 sesiones de una hora, ha contado con la participación de 62 alumnos, mientras que la participación en el grupo de control, en el que no ha habido manipulación, es de 45 jóvenes.

El desarrollo de la investigación está formado por cuatro fases claramente diferenciadas: la fase I, consistente en el establecimiento del problema y de los objetivos de investigación; la fase II, relativa al pretest o fase pre-experimental; la fase III, fase experimental, en la que se implementa el plan de intervención para el desarrollo de los hábitos seguros y responsables de los jóvenes al utilizar las TIC; la fase IV, correspondiente con el postest y la valoración del plan de intervención.

Los resultados obtenidos en la fase pre-experimental permitieron conocer los hábitos seguros y responsables, previos a la implementación del plan de intervención, de los jóvenes participantes. Además, estos resultados contribuyeron a elaborar un tratamiento adecuado a las características y necesidades de los jóvenes. Posteriormente, gracias a la implementación del plan de intervención para desarrollar hábitos seguros y responsables en el uso de las TIC, se ha podido analizar el impacto del tratamiento sobre la seguridad con la que los jóvenes hacen uso de las TIC y su exposición a los riesgos analizados. Además, en el análisis de los resultados se comprobó si los alumnos que

formaron parte del grupo experimental (grupo que recibió el tratamiento) desarrollaron sus hábitos seguros y responsables al utilizar las TIC en mayor medida que aquellos que conformaron el grupo de control (grupo que no había recibido ningún tipo de intervención específica). Con todo ello, se pretendió determinar la idoneidad del programa.

"Si el mundo cambia y tú no lo haces,

estarás viviendo en un mundo que no existe"

Alfredo Vela

Agradecimientos

A centros educativos y alumnos participantes, sin ellos no hubiera sido posible esta investigación.

A la Fundación Balia, por su inestimable apoyo en el transcurso de la investigación y por su esfuerzo por construir un mundo mejor, en el que los jóvenes puedan disfrutar de las TIC sin exponerse a los riesgos que derivan de su uso.

A las personas que han confiado en mí, familia y amigos, apoyándome y ayudándome a lo largo de estos años de trabajo.

A mi madre, Mercedes, por mostrarme el camino a seguir y apoyarme en todas las decisiones que he tomado a lo largo de mi vida. Todos mis logros son los suyos.

A Luca y Ana por darme fuerzas y hacerme sonreír cada día de mi vida.

Y, mi más sincero agradecimiento a Melchor Gómez García, mi tutor, por guiarme a lo largo de este proceso y compartir conmigo su tiempo, conocimientos y sabiduría.

ÍNDICE

CAPÍTULO I: INTRODUCCIÓN 1

1. Presentación 1

2. Riesgos derivados del uso de las TIC 4

CAPÍTULO II: MARCO TEÓRICO 8

1. Hábitos nocivos en el uso de las TIC 8

2. Iniciativas europeas para la creación de una Internet segura para los menores ... 62

2.1 EU Kids Online I 62

2.2 EU Kids Online II 77

2.3 EU Kids Online III (2011-2014) 95

2.4 La industria en internet: Coalición CEO 103

2.5 Net Children Go Mobile 121

2.6 Agenda digital para Europa 134

2.7 Estrategia europea 'Una mejor internet para los niños' 145

2.8 Agenda digital en Europa 168

3. Iniciativas españolas para la creación de una Internet segura para los menores 182

3.1 INFOXXI 182

3.2 España.es 184

3.3 Plan Avanza 187

3.4 Plan avanza 2 (2011 – 2015) 208

3.5 La Agenda Digital en España 218

4. Otras iniciativas relevantes en la seguridad on line de los menores 229

4.1 eNACSO (European NGO Alliance for Child Safety On line) 229

4.2 Protégeles 230

4.3 Red.es 231

4.4 INTECO e INCIBE 232

4.5 Oficina de Seguridad del Internauta 234

5. Ley orgánica para la mejora de la calidad educativa y real decreto por el que se establece el currículo de la enseñanza secundaria obligatoria 237

6. Leyes y normativas españolas relativas a la seguridad en Internet 246

CAPÍTULO III. DISEÑO METODOLÓGICO 253

1. Planteamiento del problema de investigación 253

1.1 Objeto de estudio 253

1.2 Valoración del objeto de estudio 255

1.3 Objetivos 259

1.4 Hipótesis 259

1.5 Variables 261

1.6 Formas de control de las variables: validez interna del experimento 263

2. Diseño de la investigación 266

3. Procedimiento 270

3.1 FASE I: establecimiento del problema y de los objetivos de la investigación 270

3.2 FASE II: pretest 272

3.3 FASE III: planificación e implementación del plan de intervención 274

3.4 FASE IV: postest 276

4. Ética de la investigación 278

5. Instrumentos de evaluación 279

6. Plan de análisis 295

CAPÍTULO IV. ANÁLISIS ESTADÍSTICO Y RESULTADOS 300

1. Introducción 300

2. Fase pre-experimental 301

2.1 Condiciones de partida del grupo experimental y grupo de control 302

2.2. Síntesis del análisis de los resultados del pretest 367

3. Fase Postest: Impacto del plan de intervención 374

3.1. Análisis de las diferencias entre el pretest y el postest 374

3.2. Otros análisis relevantes del postest 400

3.3. Análisis de la influencia de la variable “género” en el postest 405

3.4. Síntesis de los resultados pretest-postest 416

CAPÍTULO V. DISCUSIÓN Y CONCLUSIONES 427

1. Discusión 427

2. Conclusiones 433

3. Limitaciones del estudio 439

4. Aportaciones y líneas futuras de investigación 441

5. Síntesis 446

CAPÍTULO VI: REFERENCIAS 448

CAPÍTULO VII: ANEXOS 466

ÍNDICE DE FIGURAS

Figura 1 Fases cibergrooming 21

Figura 2 Princesa Lorelei ProANA (LORELEI, P, 2015) 41

Figura 3 Imágenes ProANA y ProMIA 43

Figura 4 Protocolo denuncia (Fundacion imagen y autoestima, 2013) 46

Figura 5 Formulario de denuncia apología de la anorexia y la bulimia (Asociación Contra la Anorexia y la Bulimia de Cataluña, 2015) 46

Figura 6 Número de estudios realizados en cada país 64

Figura 7 EU Kids Online: Focus del Proyecto 66

Figura 8 Riesgos relacionados con el uso de los y las menores en Internet. 68

Figura 9 Clasificación de países por uso de Internet y exposición a los riesgos. 70

Figura 10 1Correlación por países entre restricción y mediación de los padres en el uso de Internet de sus hijos e hijas..... 73

Figura 11 Países participantes en el Euro Kids On Line II..... 79

Figura 12 Posibles consecuencias de las actividades on line..... 80

Figura 13 Relaciones de uso, actividades, y factores de riesgo que pueden dañar al menor 83

Figura 14 Uso de los dispositivos con acceso a Internet 85

Figura 15 Datos sobre las habilidades en la red que poseen los menores 88

Figura 16 Riesgos percibidos por los menores en la red según grupos de edad. 90

Figura 17 Percepción del daño por parte de los menores 91

Figura 21 Países participantes en EU Kids Online III 96

Figura 22 Riesgos que encuentran los jóvenes en Internet 108

Figura 23 Menores que usaron las herramientas de denuncia satisfactoriamente 110

Figura 24 Uso de las herramientas de privacidad en las redes Sociales 112

Figura 25 Herramienta You Rate It 118

Figura 26 Herramienta You Rate It 119

Figura 27 Ciclo virtuoso de la economía digital 137

Figura 28 Celebración 'Día mundial por un Internet seguro' 149

Figura 29 Número de países que celebran el 'Día mundial por un Internet seguro' 150

Figura 30 Países pertenecientes a la red Insafe 155

Figura 31 Convergencia de los agentes por la seguridad de los jóvenes en Internet 156

Figura 32 líneas de denuncia coordinadas con INHOPE 164

Figura 33 Web Fundación Alia2 166

Figura 34 Líneas maestras España.es 185

Figura 35 Objetivos Educación en la Era Digital 190

Figura 36 Objetivos el Nuevo Contexto Digital e-Confianza 192

Figura 37 Objetivos Educación en la Era Digital 193

Figura 38 Presupuesto 2008 para desarrollo Sociedad de la Información 198

Figura 39 Impacto cuantitativo de las actuaciones desde el año 2004 al 2008 207

Figura 40 Crecimiento sector TIC 209

Figura 41 Cambios contribución VAB 210

Figura 42 Iniciativas por bloques del Plan Avanza 2 216

Figura 43 Fondos movilizados 216

Figura 44 Comparativa de las inversiones 217

Figura 45 Inversión Madrid 218

Figura 46 Áreas de trabajo Red.es 232

Figura 47 Resumen de investigación 265

Figura 48 Temporalización 275

Figura 49 Items Pretest 284

Figura 50 Items Postest..... 287

Figura 51 Asociación Infomación Pretest..... 298

Figura 52 Asociación Infomación Postest..... 299

ÍNDICE DE TABLAS

Fase pre-experimental

Tabla 1 Contingencia género 302

Tabla 2 Pruebas de Chi-cuadrado género 303

Tabla 3 Prueba de Kolmogorov-Smirnov 303

Tabla 4 Informe edad 304

Tabla 5 Rangos edad 304

Tabla 6 Contingencia información previa hábitos seguros y responsables 305

Tabla 7 Pruebas de chi-cuadrado información previa hábitos seguros y responsables 305

Tabla 8 Contingencia contactos en RRSS 306

Tabla 9 Pruebas de Chi-cuadrado contactos RRSS 307

Tabla 10 Distribución fotos personales en RRSS 307

Tabla 11 U de Mann-Whitney fotos personales en RRSS 308

Tabla 12 Contingencia percepción fotos inadecuadas 308

Tabla 13 Pruebas de chi-cuadrado percepción fotos inadecuadas 308

Tabla 14 Contingencia percepción comentario inadecuado 309

Tabla 15 Pruebas de chi-cuadrado percepción comentario inadecuado 310

Tabla 16 Contingencia configurar privacidad 310

Tabla 17 Pruebas de chi-cuadrado configurar privacidad. 311

Tabla 18 Contingencia compartir fotos o vídeos con amigos..... 311

Tabla 19 Pruebas de chi-cuadrado compartir fotos o vídeos con amigos..... 312

Tabla 20 Contingencia compartir fotos o vídeos con amigos de mis amigos 312

Tabla 21 Pruebas de chi-cuadrado compartir fotos o vídeos con amigos de mis amigos 313

Tabla 22 Contingencia compartir fotos o vídeos con conocidos en internet..... 313

Tabla 23 Pruebas de chi-cuadrado compartir fotos o vídeos con conocidos en internet 314

Tabla 24 Predisposición a compartir e-mail con personas conocidas en internet 314

Tabla 25 Prueba chi-cuadrado predisposición a compartir e-mail con personas conocidas en internet..... 315

Tabla 26 Contingencia predisposición a compartir teléfono desconocidos..... 315

Tabla 27 Prueba chi-cuadrado predisposición a compartir teléfono desconocidos..... 316

Tabla 28 Predisposición uso de la webcam con amigos..... 316

Tabla 29 Contingencia uso de webcam con amigos..... 317

Tabla 30 Pruebas de chi-cuadrado uso de webcam con amigos..... 317

Tabla 31 Contingencia uso de webcam con amigos de mis amigos..... 318

Tabla 32 Pruebas de chi-cuadrado uso de webcam con amigos de mis amigos 318

Tabla 33 Contingencia uso de la webcam con conocidos en internet 319

Tabla 34 Pruebas de chi-cuadrado uso de webcam con conocidos en internet 319

Tabla 35 Contingencia burlarse de una foto o comentario 320

Tabla 36 Pruebas de chi-cuadrado de contingencia burlarse de una foto o comentario 320

Tabla 37 Contingencia uso software de protección en el ordenador 321

Tabla 38 Pruebas de chi-cuadrado uso software de protección en el ordenador 321

Tabla 39 Contingencia uso software de protección en el Smartphone 322

Tabla 40 Pruebas de chi-cuadrado uso software de protección en el Smartphone 322

Tabla 41 Prueba de Kolmogorov-Smirnov escala Likert 323

Tabla 42 Informe descriptivo escala Likert 324

Tabla 43 Estadísticos de contraste escala Likert 325

Análisis de la influencia de la variable "género"

Tabla 44 Contingencia contactos en RRSS 327

Tabla 45 Prueba chi-cuadrado contacto en RRSS 328

Tabla 46 Informe fotos compartidas en RRSS 328

Tabla 47 Prueba U de Mann-Whitney fotos personales en RRSS 328

Tabla 48 Contingencia percepción fotos inadecuadas en RRSS 329

Tabla 49 Pruebas de chi-cuadrado percepción fotos inadecuadas en RRSS 329

Tabla 50 Contingencia percepción comentarios inadecuados en RRSS..... 330

Tabla 51 Pruebas de chi-cuadrado percepción comentarios inadecuados en RRSS.... 330

Tabla 52 Contingencia configuración seguridad y privacidad en RRSS..... 331

Tabla 53 Pruebas de chi-cuadrado configuración seguridad y privacidad en RRSS... 331

Tabla 54 Contingencia predisposición compartir fotos o vídeos personales con amigos 332

Tabla 55 Pruebas de chi-cuadrado predisposición compartir fotos o vídeos personales con amigos..... 332

Tabla 56 Contingencia predisposición compartir fotos o vídeos con amigos de mis amigos 333

Tabla 57 Pruebas de chi-cuadrado predisposición compartir fotos o vídeos con amigos de mis amigos..... 333

Tabla 58 Contingencia compartir fotos/vídeos con conocidos en internet-género..... 334

Tabla 59 Pruebas de chi-cuadrado compartir fotos/vídeos con conocidos en internet-género 334

Tabla 60 Contingencia predisposición a compartir e-mail con desconocidos..... 335

Tabla 61 Prueba Chi-cuadrado predisposición a compartir e-mail con desconocidos 335

Tabla 62 Contingencia predisposición a compartir nº de teléfono con desconocidos . 336

Tabla 63 Prueba chi-cuadrado predisposición a compartir nº de teléfono con desconocidos 336

Tabla 64 Contingencia predisposición uso de webcam con amigos..... 337

Tabla 65 Pruebas de chi-cuadrado predisposición uso de webcam con amigos..... 337

Tabla 66 Contingencia predisposición uso de la webcam con amigos de amigos 338

Tabla 67 Pruebas de chi-cuadrado predisposición uso de la webcam con amigos de amigos 338

Tabla 68 Contingencia predisposición uso de la webcam con conocidos en internet . 339

Tabla 69 Pruebas de chi-cuadrado predisposición uso de la webcam con conocidos en internet..... 339

Tabla 70 Contingencia humillación a terceros en RRSS..... 340

Tabla 71 Pruebas de chi-cuadrado humillación a terceros en RRSS..... 340

Tabla 72 Contingencia uso de software de protección en el ordenador 341

Tabla 73 Pruebas de chi-cuadrado uso de software de protección en el ordenador 341

Tabla 74 Contingencia uso de software de protección en el smartphone..... 342

Tabla 75 Pruebas de chi-cuadrado Uso de software de protección en el smartphone . 342

Tabla 76 Estadísticos descriptivos escala Likert 343

Tabla 77 Prueba U de Mann-Whitney escala de Likert..... 345

Análisis de la influencia de la variable Información previa hábitos seguros y responsables

Tabla 78 Contingencia contactos en RRSS 346

Tabla 79 Prueba Chi-cuadrado contactos en RRSS..... 347

Tabla 80 Informe fotos personales compartidas en RRSS 347

Tabla 81 Prueba U de Mann-Whitney fotos compartidas en RRSS..... 348

Tabla 82 Contingencia percepción fotos inadecuadas en RRSS 348

Tabla 83 Pruebas de chi-cuadrado percepción fotos inadecuadas en RRSS 349

Tabla 84 Contingencia percepción comentario inadecuado en RRSS..... 349

Tabla 85 Pruebas de chi-cuadrado percepción comentario inadecuado en RRSS..... 350

Tabla 86 Contingencia configuración seguridad y privacidad en RRSS..... 350

Tabla 87 Pruebas de chi-cuadrado configuración seguridad y privacidad en RRSS... 351

Tabla 88 Contingencia predisposición a compartir fotos o vídeos personales con amigos 352

Tabla 89 Pruebas de chi-cuadrado predisposición a compartir fotos o vídeos personales con amigos..... 352

Tabla 90 Contingencia predisposición a compartir fotos o vídeos personales con amigos de mis amigos..... 353

Tabla 91 Pruebas de chi-cuadrado predisposición a compartir fotos o vídeos personales con amigos de mis amigos 353

Tabla 92 Contingencia predisposición a compartir fotos o vídeos personales con personas conocidas en internet 354

Tabla 93 Pruebas de chi-cuadrado predisposición a compartir fotos o vídeos personales con personas conocidas en internet 354

Tabla 94 Contingencia predisposición a compartir el e-mail con desconocidos 355

Tabla 95 Prueba chi-cuadrado predisposición a compartir el e-mail con desconocidos 356

Tabla 96 Contingencia predisposición a compartir el teléfono con desconocidos 356

Tabla 97 Prueba chi-cuadrado predisposición a compartir el teléfono con desconocidos 357

Tabla 98 Contingencia predisposición uso de la webcam con mis amigos 357

Tabla 99 Pruebas de chi-cuadrado predisposición uso de la webcam con mis amigos 358

Tabla 100 Contingencia predisposición uso de la webcam con amigos de mis amigos 358

Tabla 101 Pruebas de chi-cuadrado predisposición uso de la webcam con amigos de mis amigos 359

Tabla 102 Contingencia predisposición uso de la webcam con conocidos en internet 359

Tabla 103 Pruebas de chi-cuadrado predisposición uso de la webcam con conocidos en internet 360

Tabla 104 Contingencia humillación a terceros en RRSS 360

Tabla 105 Pruebas de chi-cuadrado humillación a terceros en RRSS 361

Tabla 106 Contingencia uso de software de protección en el ordenador 362

Tabla 107 Pruebas de chi-cuadrado uso de software de protección en el ordenador . 362

Tabla 108 Contingencia uso de software de protección en el Smartphone 363

Tabla 109 Pruebas de chi-cuadrado uso de software de protección en el Smartphone 363

Tabla 110 Estadísticos descriptivos variables escala Likert 364

Tabla 111 Prueba U de Mann-Whitney variables escala Likert 365

Fase Postest: Impacto del plan de intervención

Tabla 112 Informe descriptivo impacto contactos en RRSS 375

Tabla 113 Prueba Wilcoxon impacto contactos en RRSS 375

Tabla 114 Contingencia impacto percepción fotos inadecuadas en RRSS 376

Tabla 115 Chi-cuadrado fotos inadecuadas en RRSS 377

Tabla 116 Contingencia impacto en la percepción comentarios inadecuados en RRSS 378

Tabla 117 Chi-cuadrado impacto percepción comentarios inadecuados en RRSS 379

Tabla 118 Contingencia impacto configuración seguridad y privacidad en RRSS 379

Tabla 119 Chi-cuadrado impacto configuración seguridad y privacidad en RRSS 380

Tabla 120 Contingencia predisposición a compartir fotos o vídeos personales con amigos 381

Tabla 121 Chi-cuadrado impacto predisposición a compartir fotos o vídeos personales con amigos..... 382

Tabla 122 Contingencia predisposición a compartir fotos o vídeos personales con amigos de amigos 382

Tabla 123 Pruebas de chi-cuadrado predisposición a compartir fotos o vídeos personales con amigos de amigos..... 383

Tabla 124 Contingencia predisposición a compartir fotos o vídeos personales con conocidos en internet..... 384

Tabla 125 Prueba chi-cuadrado predisposición a compartir personas conocidas en internet..... 385

Tabla 126 Contingencia predisposición a compartir e-mail con desconocidos..... 385

Tabla 127 Chi-cuadrado predisposición a compartir e-mail con desconocidos 386

Tabla 128 Contingencia predisposición a compartir información con desconocidos teléfono..... 387

Tabla 129 Chi-cuadrado predisposición a compartir información con desconocidos teléfono..... 387

Tabla 130 Contingencia predisposición uso de la webcam con amigos 388

Tabla 131 Pruebas de chi-cuadrado predisposición uso de la webcam con amigos 389

Tabla 132 Contingencia predisposición uso de la webcam con amigos de mis amigos 389

Tabla 133 Pruebas de chi-cuadrado predisposición uso de la webcam con amigos de mis amigos 390

Tabla 134 Contingencia predisposición uso de la webcam con conocidos en internet 391

Tabla 135 Pruebas de chi-cuadrado predisposición uso de la webcam con conocidos en internet 391

Tabla 136 Contingencia uso software de protección en ordenador de casa 392

Tabla 137 Pruebas de chi-cuadrado uso software de protección en ordenador de casa 393

Tabla 138 Contingencia uso software de protección en Smartphone 394

Tabla 139 Pruebas de chi-cuadrado uso software de protección en Smartphone 394

Tabla 140 Estadísticos descriptivos escala Likert 395

Tabla 141 Estadísticos de contraste impacto variables escala Likert 399

Tabla 142 Fotos o vídeos eliminados tras la intervención en las RRSS 401

Tabla 143 Prueba Monte Carlo fotos eliminadas tras la intervención 401

Tabla 144 Revisión de la configuración de seguridad y privacidad de las RRSS 402

Tabla 145 Prueba chi-cuadrado revisión configuración tras la intervención..... 403

Tabla 146 Contingencia asociación variables configuración seguridad..... 404

Tabla 147 Prueba chi-cuadrado asociación variables configuración seguridad 404

Tabla 148 Contingencia relación necesidad antivirus instalación..... 405

Tabla 149 Prueba U de Mann-Whiney relación software de seguridad e instalación 405

Tabla 150 Contingencia percepción comentarios inadecuados en RRSS..... 406

Tabla 151 Chi-cuadrado percepción comentarios inadecuados en RRSS 407

Tabla 152 Contingencia predisposición Uso de la webcam con amigos..... 408

Tabla 153 Chi-cuadrado predisposición Uso de la webcam con amigos 409

Tabla 154 Estadísticos descriptivos variables escala Likert en el grupo de control.... 410

Tabla 155 U de Mann-Whitney variables escala Likert grupo de control..... 411

Tabla 156 Estadísticos descriptivos variables escala Likert en el grupo de experimental 412

Tabla 157 U de Mann-Whitney variables escala Likert grupo experimental..... 413

Tabla 158 Estadísticos descriptivos variables escala Likert en el total de la muestra. 414

Tabla 159 U de Mann-Whitney variables escala Likert total de la muestra..... 415

CAPÍTULO I: INTRODUCCIÓN

1. Presentación

La integración de las TIC en los hogares españoles ha sido progresiva, llegando a estar presentes, según estudios realizados en 2016, en el 96,7% de los hogares españoles debido a la presencia de telefonía móvil, en el 81,2% si nos referimos a la conexión de banda ancha o en el 77,1% en aquellos que disponen de algún dispositivo de conexión a internet (Instituto Nacional de Estadística, 2016).

Las TIC están presentes en las vidas de todas las personas, directa o indirectamente. Por supuesto, no todas las TIC son útiles o necesarias para todas las personas, sin embargo, debido a la gran variedad de posibilidades que nos ofrecen, es más que probable que cualquier persona, con independencia de la edad, sexo, ideología o cultura, pueda encontrar beneficios en ellas. Tal y como dijo el ex-secretario general de la ONU, Kofi Annan (2003): «Las tecnologías de la información y la comunicación no son ninguna panacea ni fórmula mágica, pero pueden mejorar la vida de todos los habitantes del planeta.»

Las oportunidades de ocio y socialización que ofrecen las TIC han hecho que los más jóvenes se sientan atraídos por ellas (Protegeles, 2009), lo cual ha propiciado que desarrollen grandes habilidades digitales que les permiten aprovechar sus beneficios y oportunidades.

Sin embargo, no todo lo aportado por las TIC son buenas noticias. Paralelamente a su desarrollo tecnológico, se han detectado situaciones o fenómenos

que pueden suponer un peligro para el usuario de las TIC si no se toman las precauciones adecuadas. (INTECO, 2009, pág. 70)

Los niños y jóvenes, nativos digitales, han nacido inmersos en la Sociedad de la Información, en la que participan activamente aprovechando al máximo sus posibilidades de comunicación y socialización. De forma paralela al avance de las TIC, aparecen escenarios que pueden generar situaciones de riesgo para los menores, los cuales han sido capaces de adquirir ciertas habilidades tecnológicas que les permiten hacer uso de las herramientas digitales que consideran útiles pero, sin embargo, no han sido capaces de desarrollar del mismo modo los hábitos seguros y responsables cuando hacen uso de las TIC (INTECO, 2009).

Internet, que no fue creada inicialmente para el uso de menores, aporta elementos que resultan atrayentes y motivadores, como el anonimato, la capacidad de socializarse y sentirse miembro de un grupo, la construcción de identidades, la inmediatez, la accesibilidad, etc. (Sánchez-Carbonell y Beranuy, 2007). Por su parte, el móvil brinda la oportunidad de estar en contacto permanente, socializarse, disfrutar del ocio, generar seguridad y una sensación de control a los padres y parejas, asumir autonomía, proporcionar intimidad, favorecer la conciliación familiar, facilitar la gestión del tiempo y de la información (Beranuy y Sánchez-Carbonell, 2007).

En los centros educativos, las competencias digitales han ido adquiriendo mayor importancia en el currículo del centro, no obstante, la velocidad con la que los jóvenes desarrollan habilidades tecnológicas avanza paralelamente a una gran carencia o vulnerabilidad, al no desarrollarse con la misma velocidad los hábitos seguros y responsables durante su utilización.

Hoy, podemos constatar que los distintos usos de Internet y en general de las redes sociales, por niños y jóvenes genera constantes discursos y acciones de distinto tipo (políticas, legales, pedagógicas) para contrarrestar los riesgos reales y potenciales que tienen preocupados a distintas audiencias de la sociedad. Livingstone (2007) que dirigió EU Kids Online, expone que los riesgos derivados del uso de las TIC supone, para los niños y adolescentes, la exposición a daños potenciales para su seguridad, bienestar y desarrollo. Lamentables sucesos en el mundo entero y los resultados de los estudios realizados en Europa, y más concretamente en España, corroboran la opinión de los expertos reafirmando la urgente necesidad de generar hábitos seguros, saludables y responsables en el uso de las TIC por los niños y jóvenes.

2. Riesgos derivados del uso de las TIC

Los riesgos asociados al uso de las TIC son muy diversos, además de dinámicos. No hablamos de riesgos estáticos e impasibles, sino que decimos que los riesgos evolucionan del mismo modo que evolucionan las TIC. Los riesgos que hoy son detectados, necesariamente, no han de ser los mismos de mañana. Con la evolución de las tecnologías de la información y la comunicación aparecen nuevos riesgos, algunos de los cuales son reducidos y/o eliminados rápidamente gracias a programas creados con este fin, como los antivirus, sin embargo no todos los riesgos es posible eliminarlos tan fácilmente, sino que depende del uso y responsabilidad que el usuario de a las TIC que estén protegidos (INTECO, 2009)

La responsabilidad en el uso de un instrumento no es nada nuevo en nuestra sociedad: disponemos de enchufes por los que pasa corriente eléctrica que fácilmente podrían suponer un peligro para niños y adultos, pero aprendimos a utilizarlos sin riesgo; disponemos de cuchillos que hasta los más pequeños aprenden a usar sin cortarse; disponemos también de automóviles,…etc. Del mismo modo que hemos aprendido a utilizar diferentes herramientas, dispositivos u otros artefactos que mal usados tienen un gran peligro, hemos adquirido el hábito de utilizarlos con precaución, por lo que no es descabellado transmitir, de todos los modos que se nos ocurran, que la utilización de las TIC requieren responsabilidad y conocimientos sobre sus usos y peligros. (Sanz Mamolar y Ramos Sancha, 2012)

Los riesgos derivados del uso de las TIC pueden afectar a diferentes colectivos o grupos sociales que pueden resultar especialmente vulnerables ante estos fenómenos.

Según los expertos, los más jóvenes, niños y adolescentes, debido a su adopción natural de las TIC, pueden ser más proclives a asumir riesgos (o determinados tipo de riesgos, como aquellos que tienen que ver con la publicación de datos personales) que los adultos, más cautelosos y recelosos (International Working Gourp on Data Protection in Telecomunications, 2008). En este sentido los adolescentes son vulnerables debido a algunas características propias de esta etapa evolutiva, como son: la necesidad de establecer relaciones sociales, la baja autoestima, escasa valoración de sus datos o información personal, etc., pudiendo realizar acciones que puedan suponer un riesgo para ellos mismos. (INTECO, 2009, pág. 80)

Los peligros procedentes del uso de las TIC, analizados en su mayoría por INTECO en el 2009 en la investigación 'Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres', son los siguientes:

- Tecnoadicción: es la patología motivada por la dependencia de un determinado dispositivo o servicio tecnológico. Puede estar relacionada o desencadenar adicciones paralelas tales como ludopatía on line, adicción al sexo, FOMO (miedo a perderse algo) por lo que la persona está constantemente revisando su red social, compra on line de manera compulsiva, etc. (Flores Fernández, 2008)

- Ciberbullying: consiste en el acoso o intimidación a través de las tecnologías de la información y la comunicación. Se realiza a través de mensajes de texto de teléfonos móviles, correos electrónicos, llamadas telefónicas, salas de chat de Internet, mensajería instantánea o a través de las servicios de redes sociales (Webster, 2011). Cuando hablamos de ciberbullying, nos referimos únicamente a la existencia de acosado y acosador en una relación entre iguales, es decir,

entre personas de edad cercana entre sí (INTECO, 2009, pág. 78).

- Cibergrooming, grooming: son las acciones llevadas a cabo por adultos, a través de Internet, para ganarse la confianza de un/a menor con la intención de obtener beneficios sexuales. El cibergrooming, en ocasiones, es la antesala del abuso sexual (PantallasAmigas, 2012).

- Sexting: envío de contenidos eróticos o pornográficos por medio de teléfonos móviles (Defensor del menor, 2011).

- Sextorsión: consiste en realizar coacción y/o chantaje a partir de fotos robadas u obtenidas mediante sexting (Wikipedia, 2013).

- Vulneración de derechos de propiedad intelectual: descargas ilegales de videos, música, video-juegos, programas informáticos, etc. (INTECO, 2009)

- Acceso a contenidos inapropiados: una de las principales ventajas que ofrece el acceso a la red es el acceso a todo tipo de contenidos. Ésta es a la vez uno de sus principales y más frecuentes riesgos si se trata de un menor (INTECO, 2009).

- Amenazas a la privacidad: Robo, publicación y difusión de datos e imágenes personales. La obtención de nuestra información privada no se obtiene únicamente mediante la substracción sino que en ocasiones en proporcionada por los mismo usuarios a través de Internet (INTECO, 2009).

- Amenazas técnicas, virus y fraudes: el uso de la red nos expone al ataque de virus u otros programas informáticos, malware, con fines maliciosos. Las consecuencias pueden ser inmediatas, como la pérdida de información, o la ralentización del sistema, robo de información personal y fotografías, etc. Los

fraudes tienen por objeto provocar un perjuicio económico al usuario que se derivan de compras, subastas, apuestas, juegos de azar, etc. (INTECO, 2009).

CAPÍTULO II: MARCO TEÓRICO

1. Hábitos nocivos en el uso de las TIC

a) Tecnoadicción

Se conoce como tecnoadicción a la patología motivada por la dependencia de un determinado dispositivo o servicio tecnológico. Puede estar relacionada o desencadenar adicciones paralelas como ludopatía on line, adicción al sexo, FOMO (miedo a perderse algo) por lo que la persona está constantemente revisando su red social, compras on line de manera compulsiva, etc. (Flores Fernández, 2008). Incluye todos aquellos fenómenos o problemas de abuso a las TIC. Puede darse adicción al teléfono móvil o Smartphone, a la mensajería instantánea, videojuegos, etc. (Pantallas Amigas, 2009).

El impacto de las TIC, como Internet y el Smartphone, es tan espectacular que es lícito preguntarse si, en algunos casos, pueden provocar adicción, al igual que otras conductas socialmente aceptadas como comprar, jugar, trabajar y practicar sexo (Alonso-Fernández, 2003; Echeburúa, 1999; González Duro, 2005; Holden, 2001; Lemon, 2002). Además, "como toda adicción, Internet puede ser el detonante de otros problemas (depresión, ansiedad, ludopatía, etc.). El uso excesivo puede vincularse con la calma de un malestar, obteniendo alivio inicialmente, pero después vuelve el malestar y entonces se genera la tolerancia: necesito aumentar el uso para lograr el mismo efecto", explica Laura Jurkowski, directora de un centro argentino especializado en este tipo de ciberdependencia. Australia fue el primer país en agregar la adicción a

Internet a su manual de psiquiatría en 2012.

El uso excesivo puede llegar a interferir con otras actividades cotidianas y hasta perturbar sus relaciones sociales y familiares. En el caso que, además, el usuario sea incapaz de dejar de usar Internet, o que le produzca un enorme malestar cuando no se puede conectar, podemos encontrarnos frente a un problema de adicción (Chóliz y Marco, 2012).

Situación de la exposición al riesgo

El informe de Eu Kids Online II muestra, en su análisis de los datos obtenidos de 25 países participante, que un 29% de los menores han experimentado uno o más de los cinco componentes asociados con un excesivo uso de Internet, aunque tan solo un 1% muestra niveles patológicos de uso (Garmendia, Garitaonandia, Martínez, & Casado, 2011).

Garmendia et al. (2011) encontraron que el 12% de los jóvenes se ha quedado en alguna ocasión sin dormir por usar Internet, de los que el 8% lo hacen a menudo. El 8% dicen pasar menos tiempo con la familia, amigos o haciendo tareas escolares, por estar conectado a Internet, y el 4% afirman haberse quedado sin comer por usar Internet.

Un estudio realizado en China (Ligang, y otros, 2013) a 10982 jóvenes de edades comprendidas entre los 13 y los 23 años obtuvo una tasa de prevalencia de adicción a Internet del 7,5%. En el estudio se observa, además, la relación existente entre la adicción a Internet y el bienestar de la persona. El aumento de los síntomas de consumo adictivo se asoció con la disminución de la autoestima, la satisfacción por la

vida y el aumento de la depresión. En el estudio publicado por Minetur (2014) llamado 'Encuesta sobre hábitos de uso y seguridad de Internet de menores y jóvenes en España', se obtiene que el 22,5% de los jóvenes encuestados pasan más de tres horas al día utilizado Internet, aunque no lo relaciona con tecnoadicción.

El periódico ABC en un artículo de 2015 titulado '¿Eres un adicto?' ha entrevistado a Luque y Emanuel Aramburu quien, en su proyecto de Doctorado, ha elaborado un instrumento de medición que dice detectar la adicción a la tecnología. La escala diagnóstica de adicción a la tecnología consta de 37 afirmaciones entre las que figuran las siguientes: 'Me siento aislado cuando no tengo o no puedo usar mi teléfono móvil', 'Cuando me siento aburrido o solo, comienzo a enviar SMS', 'Siento que me falta algo cuando la computadora no está encendida', 'Solo cuando uso Internet (ej: Facebook) me puedo olvidar de situaciones desagradables', etc.

FOMO

En la sociedad en la que vivimos, si algo nos define es "vivir acelerados". No sólo corremos para llegar a tiempo al trabajo, también corremos para quedar con un amigo, para ir a comer o para llegar a ver un película. Da igual que sea en nuestra vida profesional o en nuestro tiempo libre, sentimos la necesidad de aprovechar el tiempo al máximo, no queremos sentir que no lo aprovechamos todo lo posible o sentir que perdemos la oportunidad de hacer otras cosas más interesantes.

Con la llegada de las redes sociales, compartir fotos o información de momentos felices vividos en cualquier ámbito de nuestra vida, ya sea profesional o, especialmente, privada, se ha convertido en una actividad habitual. En muchos casos

se realiza a diario, en otros incluso varias veces en el mismo día. La información compartida, normalmente, suele coincidir con momentos felices de viajes, comidas suculentas, fiestas con amigos, etc., nadie comparte una foto de una discusión en pareja. Es por ello, que las redes sociales multiplican la idealización de la vida. "El bienestar que creemos percibir en los demás puede llevarnos tanto a la envidia como a la depresión", dice el psicólogo Jesús Gabriel Gutiérrez.

De este modo, cuando un usuario se sienta frente a una red social puede sentirse muy desgraciado. Esta sensación es la que se ha denominado FOMO (fear of missing out) o lo que es lo mismo "miedo a perderse algo".

El FOMO no es exclusivo de las redes sociales, ni siquiera es algo nuevo, según Victoria Trabazo y Fernando Azor (2011), siempre ha sido bastante común, especialmente en los ambientes socioeconómicos elevados, en los que existe la necesidad de tener lo último, ya sea en moda, tecnología, coches, etc.

Este sentimiento se ha incrementado notablemente también con la llegada de los Smartphones, debido a la mayor disposición y accesibilidad de la información, así como con el software de mensajería instantánea, como el WhatsApp, en el que se comparte información del mismo tipo que la descrita a través de los grupos de contactos.

Un trastorno relativamente reciente es el de Crackberries consistente en revisar constantemente si se han recibido nuevos mensajes en el teléfono móvil con conexión a Internet. Algunas personas llegan comprobar su teléfono móvil más de 400 veces al día (La razón, 2013).

Consecuencias de las tecnoadicción

El uso excesivo de las tecnologías de la información y la comunicación supone (Protégeles, 2013):

- Deseo urgente de repetir la conducta, de volver a utilizar las TIC.
- Estado emocional negativo cuando se interrumpe la actividad (ansiedad, cambios de humor, impaciencia, irritabilidad…).
- Placer, alivio o euforia cuando se repite la conducta.
- Necesidad de incrementar progresivamente el tiempo que emplea en su uso.
- Deterioro de las relaciones sociales y familiares. Aislamiento.
- Deterioro en el rendimiento escolar o familiar.
- Problemas físicos derivados de la falta de sueño (fatiga, debilitamiento del sistema inmunitario…) y de ejercicio físico.
- Etc.

El objetivo del tratamiento de la adicción a las TIC, a diferencia de lo que ocurre con otros tratamientos de deshabituación, debe ser el uso controlado de lo que causa la adicción (Echeburúa Odriozola y de Corral Gargall, 2010, pág. 91).

Prevención

La prevención de la tecnoadicción deber ser realizada en casa por los padres y en la escuela, para obtener mayores garantías de éxito. Algunas de las estrategias de prevención recomendadas en estudios previos (Echeburúa Odriozola y de Corral

Gargall, 2010, pág. 94) son:

- Limitar el uso de aparatos y pactar las horas de uso de las TIC.
- Fomentar la relación con otras personas.
- Potenciar la lectura, el cine y otras actividades culturales.
- Estimular el deporte y las actividades en equipo.
- Desarrollar actividades grupales, como las vinculadas al voluntariado.
- Estimular la comunicación y el diálogo intrafamiliar.

b) Ciberbullying

El ciberbullying, o acoso cibernético, consiste en la intimidación a través de las tecnologías de la información y la comunicación, medios tales como mensajes de texto de teléfonos móviles, correos electrónicos, llamadas telefónicas, salas de chat de Internet, mensajería instantánea o a través de las servicios de redes sociales (Webster, 2011). Cuando hablamos de ciberbullying, nos referimos únicamente a la existencia de acosado y acosador en una relación entre iguales, es decir, entre personas de edad cercana entre sí (INTECO, 2009, pág. 78).

Hinduja y Patchin (2009) precisan el ciberbullying como "el daño intencional y repetido, infligido por parte de un menor o grupo de menores hacia otro menor mediante el uso de medios digitales". Además, nos aclaran los conceptos introducidos en la definición del fenómeno:

- Daño: la víctima sufre un deterioro de su autoestima y dignidad personal, dañando su estatus social, provocándole victimización psicológica, estrés

emocional y rechazo social.

- Intencional: el comportamiento es deliberado, no accidental, aunque no implica la intención de dañar a la otra persona.

Las ventajas para la socialización, la deslocalización y la desincronización en la comunicación, facilitan el contacto con personas conocidas o desconocidas, de mi entorno o de cualquier lugar del mundo.

Uno de los riesgos derivados de las oportunidades de socialización que ofrecen las TIC, es que facilitan que unas personas puedan ser acosadas por otras. Es decir, que el acosador, usando las TIC como medio para amenazar, intimidar o provocar a su víctima mediantes rede sociales, mensajería instantánea, videojuegos, etc.

La llegada de los Smartphones ha incrementado la comunicación a través de la red de datos entre los jóvenes y el ciberbullying entre menores (Mascheroni & Cuman, 2014). Esto se debe a la facilidad para la comunicación on line que añaden los dispositivos móviles, lo que indirectamente agrava las situaciones de ciberbullying, facilitando el contacto víctima y acosador. Lo que antes del Smartphone suponía comunicación ocasional, más o menos frecuente, ahora se puede producir constantemente durante 24 horas del día, los siete días de la semana.

El ciberbullying se puede dar en diferentes contextos como redes sociales privadas, correo electrónico, grupos de WhatsApp u otro software de mensajería instantánea, salas de juegos on line, foros, blogs, etc.

El ‘Monográfico de ciberacoso escolar (Ciberbullying)’ elaborado por Chaval.es describe exhaustivamente el Ciberbullying, aportando información que analizaremos a

continuación.

Existen diferentes métodos y medios por los que un joven puede sufrir ciberbullying, que varían por las tendencias de comunicación del momento:

- Ataques directos: insultos o amenazas enviadas a la víctima, robo de información privada como contraseñas, datos de acceso, etc.
- Publicaciones y ataques públicos: publicar rumores para dañar la imagen de la víctima, mensajes hirientes, fotos o vídeos humillantes en redes sociales, mostrar rechazo públicamente, etc.
- Ciberbullying mediante terceros: uso de otras personas para acosar a la víctima. Suplantación de identidad y creación de perfiles falsos en redes sociales o juegos on line, para ganarse la confianza de la víctima con la identidad falsa y posteriormente humillarla públicamente, o para simplemente exponerla ante el resto de usuarios y humillarla.

En las labores de sensibilización con jóvenes y familias sobre el ciberbullying es necesario que se conozcan que, además de las víctimas y acosadores, otros muchos jóvenes adquieren el rol del "espectadores" que se pueden implicar activamente sobre el suceso agravándolo o defendiendo a la víctima, o bien, actuar como sujetos pasivos consintiendo lo que ocurre sin implicarse de ningún modo.

Es necesario que estos roles intervengan en dinámicas en las aulas para concienciar a los jóvenes del valor que tienen todos y cada uno de los comportamientos. También se ha encontrado relación entre acosados y acosadores. Es decir, los acosados en muchas ocasiones se convierten en acosadores.

Principales características del ciberbullying:

- *Sentimiento de invencibilidad on line*: el anonimato puede aumentar la sensación de poder del acosador y que ésta propicie conductas abusivas. Asimismo, es bastante habitual que los comportamientos dañinos contra otros usuarios, tipificados en el ciberbullying, se vean normales y socialmente aceptados por las personas que los realizan. Además, los jóvenes y sus familias, suelen desconocer que estos actos pueden suponer un delito penal.
- *Reducción de las restricciones sociales y dificultad para percibir el daño causado*: la distancia física que permiten las TIC facilita la desinhibición de comportamientos y, en el medio digital, al no poder verse la reacción de la víctima, dificulta la percepción del daño del acosador necesario para que ponga fin a este comportamiento.
- *Siempre en contacto*: como decíamos anteriormente, la conectividad permanente permite al acosador estar presente en los tiempos personales y privados de la víctima, pudiendo ser acosado las 24 horas del día, los 7 días de la semana.
- *Viralidad*: los contenidos dañinos del acosador pueden distribuirse con gran rapidez gracias a las TIC, pudiendo convertirse en incontrolables.

Situación de la exposición al riesgo

"Diversos estudios coinciden en indicar que un 5% de los menores españoles sufren ciberacoso escolar. También se constata una ligera tendencia al alza con la edad, siendo el rango de edad entre 15 y 16 años el más significativo" (Garmendia et al., 2011).

Buelga et al. (2010) en el estudio titulado Ciberbullying: victimización entre

adolescentes a través del teléfono móvil y de Internet, cuya muestra fue de 2101 adolescentes entre 11 y 17 años, indica que, tras analizar los resultados de la investigación, un 24,6% de los adolescentes afirman haber sido acosados por el móvil en el último año, y un 29% por Internet, siendo las chicas y los estudiante de primeros cursos de ESO los más afectados.

En Europa, los datos obtenidos por la investigación Net Children Go Mobile muestran que el 8% de chicos han sufrido ciberbullying frente al 19% de chicas que consideran haber sido acosadas a través de la red. La diferencia entre chicos y chicas hace resaltar la importancia de la variable género en el estudio y en el análisis del ciberbullying. Protégeles (2014) en el estudio "Menores de Edad y Conectividad Móvil en España: Tablets y Smartphones" obtiene que el 2,4% de los niños jóvenes de 11 y 12 años, y el 8,4% de los jóvenes de 13 y 14 años han sido víctimas en burlas, amenazas o agresiones a través del Smartphone, mientras que el 2,6% de los jóvenes de 11 y 12 años y el 8,2% de los jóvenes de 13 y 14 años, han participado en acoso a otros menores. En este caso, se ha encontrado que la edad también es una variable significativa en el estudio e investigación del ciberbullying (Protégeles, 2014).

Consecuencias del ciberbullying

El ciberbullying tiene un efecto igual o más negativo en los adolescentes que el bullying tradicional y las víctimas pueden llegar a sufrir problemas psicológicos y sociológicos por mucho tiempo. Algunos daños que puede sufrir el acosado son: depresión, baja autoestima, ansiedad, alienación, intentos de suicidio, problemas de comportamiento y dificultades para concentrarse. En algunos casos, estos problemas, iniciados en la adolescencia, persisten hasta la edad adulta (Wang, Iannotti, R, &

Nansel, 2009).

Prevención

La guía del Defensor del Menor (2011) muestra un conjunto de buenas prácticas para la prevención y el tratamiento del ciberbullying:

1. La prevención y sensibilización en los buenos hábitos para evitar los abusos se debe comenzar con los más pequeños, en la educación infantil, aunque el acoso cibernético suele aparecer en la adolescencia. En este caso, es necesario tener en cuenta la edad de inicio en el uso de Internet, que ha bajado de los 11 a los 7 años. (Livingstone, Haddon, Görzig, & Ólafsson, 2010)

2. En la guía recomiendan una actividad que ha tenido éxito en repetidas ocasiones. Consiste en que los propios adolescentes, alumnos de secundaria, se conviertan en formadores en prevención de malos hábitos en el uso de las TIC con los alumnos de primaria y educación infantil.

3. La función de los padres es fundamental para la prevención de malos hábitos, por lo que es necesario acciones de sensibilización y formación con los padres de los alumnos desde una perspectiva positiva, alejada del alarmismo, centrada en las posibilidades y necesidad de las TIC por sus hijos.

Otro factor a tener en cuenta en la prevención y tratamiento en casos de ciberbullying es la relación existente entre el bullying, también conocido como acoso en las aulas, y el ciberbullying. En éste sentido, Ricardo Lucena (2003) describe el bullying como “una realidad compleja que debe abordarse desde una doble perspectiva: el propio alumno (en el que a su vez inciden variables de tipo personal, pero también

otras familiares) y el centro educativo". Por otro lado, los resultados obtenidos por Rosario del Rey, Paz Elipe y Rosario Ortega en su estudio "Bullying and ciberbullying: Overlapping and predictive value of the co-occurrence" nos muestra la relación existente entre bullying y ciberbullying. En él se observa la alta ocurrencia entre acosado y ciberacosado. Si bien un acosado tiene altas probabilidades de sufrir acoso cibernético, no ocurre lo mismo con la persona que sufre acoso cibernético primeramente para terminar siendo acosado en el aula. Esto coincide con los resultados de investigaciones anteriores (Li, 2007; Riebel, Jäger, & Fischer, 2009; Schneider, O'Donnell, Stueve, & Coulter, 2012; Smith, y otros, 2008). En definitiva, en este estudio se encontró que la victimización puede, de hecho, ayudar para predecir el ciberbullying (Gradinger, Strohmeier, & Spiel, 2009; Hemphill, y otros, 2012; Werner, Bumpus, & Rock, 2010).

Por último, el Defensor del menor (2011) ofrece una pieza fundamental para la prevención del bullying y ciberbullying: "Si algo hemos ido aprendiendo en relación al tratamiento y la gestión de los conflictos entre iguales en los centros educativos es que los propios chicos son los que mejor contribuyen a la resolución de los problemas cuando han sido formados para ello".

c) Cibergrooming o grooming

El cibergrooming engloba las acciones llevadas a cabo por adultos, a través de Internet, con la intención de obtener contenidos sexuales o algún tipo de beneficio sexual del menor, incluso pudiendo llegar al abuso sexual (PantallasAmigas, 2012). Es el ciberacoso deliberado de un adulto a un menor para establecer una relación de control sobre el menor. Utiliza un conjunto de técnicas de engaño y persuasión para disminuir

las inhibiciones del menor y obtener un beneficio de índole sexual.

Al acosador, que es mayor de edad, se le llama Cibergroomer que, a través de la comunicación on line (e-mail, redes sociales, juegos on line, chat, etc.), inicia una relación con un menor con un objetivo sexual. En las estrategias utilizadas en los casos de cibergrooming más habituales, en un principio, mostrará interés sobre los problemas o dilemas que experimenta el menor con la intención de ganarse su confianza para, más adelante, obtener imágenes, videos o video chats con contenido sexual. Es posible, que el cibergroomer intente conocer en persona al menor. (Wachs, Wolf, & Pan, 2012)

Existen dos variantes en la manera en la que el acosador inicia la relación con el menor. Por un lado tenemos la analizada por Wachs et al. (2012) en la el acoso tiene una fase previa en la que el acosador busca ganarse la confianza del menor y, la otra, en la que no existe fase previa de relación y generación de confianza sino que el acosador previamente ha encontrado el método de chantajear y coaccionar al menor. En la segunda opción, el acosador ha encontrado en la web contenidos para chantajear que él u otras personas de su entorno han subido previamente, o bien, ha hackeado su cuenta para obtenerlas. En ocasiones pueden obtener los primeros contenidos sexuales amenazándoles con el hackeo de su ordenador, es decir, haciéndoles creer que van a formatear el ordenador de la víctima o alterar el funcionamiento de algún modo.

Red.es (2015f), en el documento llamado “Monográfico Grooming”, expone las características del Cibergrooming que examinamos a continuación:

- Inicio de la relación de alguno de los modo vistos. Si busca ganarse la confianza del menor el acosador estudia y analiza previamente los gustos y preferencias del menor para establecer progresivamente una relación basada en la confianza y

comprensión.

- El objetivo es la obtención de índoles sexual, desde la obtención de imágenes, vídeos o exposición en la webcam, hasta el caso más extremo que se produzca una relación sexual física.
- En todos los casos, el chantaje es la principal arma del acosador, aunque en también se utilizan los regalos e incentivos para conseguir sus propósitos.

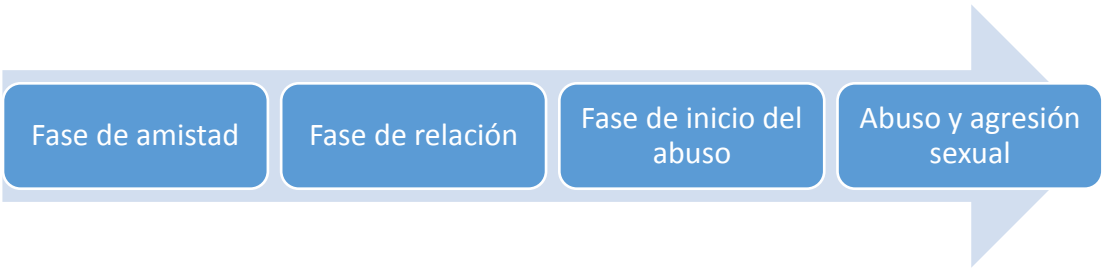


Figura 1 Fases cibergrooming

El proceso puede durar minutos, horas, días o meses, aunque, según el informe británico de "Child Exploitation and On line Protection" que evalúa la amenaza de explotación sexual a menores, la dinámica en los últimos años ha cambiado acelerándose extremadamente el proceso.

Davidson y colaboradores (2011) proponen la baja-autoestima, soledad, autolesión frente a problemas familiares como factores de riesgo que contribuyen a que el adolescente sufra cibergrooming.

Situación de la exposición al riesgo

Minetur (2014) obtiene que el 13% de los jóvenes contactan con desconocidos a través de su red social, el 8.1% por correo electrónico, el 25,4% jugando en red, el 9,9% a través de chats y el 8,3% mediante el uso de mensajería instantánea. Y concluye

afirmando que un tercio de los contactos que tienen los menores en Internet son de personas que no conocen personalmente.

Según datos de EU Kids Online II (2009-2011) el 21% de los menores afirman haber contactado en Internet con desconocidos, mientras que la media europea se sitúa en el 34%.

Aunque no implica riesgo directo de Cibergrooming, el contacto con personas por Internet, que no se conocen off line, podría ser un factor de riesgo dado que el contacto de un cibergroomer es usual que comience a través de la interacción con una persona desconocida a través de la red. Aun así, lo normal es que estos contactos sean positivos para la socialización del joven.

El cibergrooming es un fenómeno no muy conocido por la población. El INTECO, a través del estudio realizado "hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres" en 2011, obtiene que cerca de la mitad de los padres e hijos no son conscientes de este riesgo, siendo las niñas menores más conscientes del riesgo de sufrir acoso (62,2%) que los niños (39,7%).

Prevención

La universidad de Bremen (2012), a través, de un estudio elaborado por Wolak y colaboradores (2007) obtuvieron que la mayoría de los participantes hicieron frente a solicitudes de temática sexual, advirtiendo o ignorando al solicitante, evitando el chat o servicio donde le conocieron, la sala de juego o el uso del ordenador. Las estrategias para afrontar este tipo de situaciones difieren principalmente en función de del sexo, edad, tipo de riesgo interpretado, etc. (Staksrud & Livingstone, 2009).

Jorge Flores Fernández (2011) establece tres fases y diez claves de hacer frente al cibergrooming:

Fase 1: Prevención

1. No proporcionar imágenes o informaciones comprometedoras. El acosador busca obtener información de la víctima para chantajearla.
2. Evitar el robo de ese elemento. El acosador va a hacer todo lo que esté en su mano para obtener el elemento que le permita chantajear a su víctima. La seguridad del dispositivo de acceso y la confidencialidad de las contraseñas juegan un papel fundamental para impedírselo.
3. Mantener una actitud proactiva respecto a la privacidad. Es necesario prestar atención a toda la información que se publica sobre nosotros en Internet.

Fase 2: Afrontamiento:

4. No ceder bajo ningún concepto al chantaje. Si cedemos le estaremos dando mayor fuerza al acosador.
5. Pedir ayuda. Es necesario que el joven pida ayuda a un adulto de confianza que le pueda ayudar a salir de la situación de abuso.
6. Evaluar la certeza de la posesión del material que dice tener el acosador.
7. Limitar la capacidad de acción del acosador.
    - Actualizar el software de seguridad del equipo.
    - Aumentar la privacidad de mis redes sociales.
    - Si es posible, cambiar de perfil, de plataforma de juegos, chat, etc.

Fase 3: Intervención

8. Analizar las ilegalidades que ha incurrido el acosador.
9. Buscar y recopilar las pruebas de la actividad delictiva.
10. Denunciar

Desde 2010, el Código Penal español regula el cibergrooming en el artículo 183 Bis. Los expertos consideran imprescindible que, además de la prevención, estas conductas tengan una regulación penal y que jueces, fiscales y policías cuenten con los instrumentos adecuados para investigarlas (Galence, 2011). En el apartado "Leyes y normativas españolas relativas a las seguridad en Internet" se encuentra toda la información actualizada sobre las leyes que protegen a los menores en la red.

Por último, "es necesaria la coordinación desde los diferentes ámbitos (legal, medios de comunicación, institución educativa, gobiernos, empresas, etc.) para trabajar conjuntamente en la prevención de los abusos a menores" (Pulido & Flecha, 2009).

Iniciativas internacionales y nacionales, que veremos a lo largo de la investigación, luchan contra los abusos on line contra menores de carácter sexual.

Sobre cibergrooming y ciberbullying

La adolescencia es una etapa de desarrollo de la personalidad en la cual los jóvenes aprenden a afrontar situaciones de riesgo (Hurrelmann, 2010).

En una investigación realizada (Wachs, Wolf, & Pan, 2012) se observa que el género y la edad es una variable crucial en cuanto al riesgo y tipo de afrontamiento del riesgo que realizan los adolescentes. En el estudio se puede observar que las chicas

corren más riesgo que los chicos verificando lo aportado en investigaciones pasadas (Berson, 2003; Shanon, 2008; Davidson et al., 2011a). El hablar de la vida privada con extraños no es identificado como un factor de riesgo, coincidiendo con otro estudio llamado Internet-initiated sex crimes (Wolak, 2008). Estudios previos (Wolak et al., 2008; Staksrud & Livingstone, 2009; Wachs & Wolf, 2011) han demostrado que la victimización del adolescente en la vida real coincide con su victimización on line. Además, existe una fuerte relación entre las personas que han sufrido ciberbullying y las que han padecido cibergrooming.

d) Sexting

Consiste en el envío de contenidos eróticos o pornográficos por medio de teléfonos móviles. Inicialmente hacía referencia al envío de mensajes de naturaleza sexual, pero con las posibilidades que ofrecen los dispositivos móviles, han aumentado los envíos de fotografías y vídeos, a los cuales se les sigue aplicando el mismo término, aunque sexting se refiera específicamente al envío de mensajes de texto. Es una práctica cada vez más común entre adolescentes y jóvenes (Defensor del menor, 2011).

Actualmente, el sexting amplía su definición incluyendo "el envío de contenidos de tipo sexual (principalmente fotografías y/o vídeos) producidos generalmente por el propio remitente, a otras personas por medio de teléfonos móviles.", tal como podemos leer en la web www.sexting.org

Dependiendo del papel que se adquiera en la práctica del sexting está el "sexting activo" que se refiere a la persona que envía las imágenes o videos sexuales de sí mismos, y el "sexting pasivo" referido a quien recibe el contenido sexual.

Características del Sexting (Red.es, 2015e):

- Es una práctica que se realiza entre parejas como elemento de coqueteo o para captar la atención, aunque en la actualidad también es realizado entre personas desconocidas que contactan a través de redes sociales o algún software que facilite la comunicación.
- No es exclusivo de los jóvenes. También se realiza entre personas adultas.
- El principal riesgo es la pérdida de control sobre el vídeo o imagen. La persona que lo recibe puede enviárselo a terceras personas para alardear o por venganza tras la ruptura con su pareja.
- Ferguson (2011) ha relacionado el sexting en mujeres adolescentes con un mayor índice de conductas sexuales de riesgo.
- Existen factores influyentes potencialmente en el daño que puede hacer el sexting: el contenido de la imagen, que la información sea captada por el protagonista o que el protagonista otorgue permiso para su realización, la edad o si se puede identificar al sujeto en las imágenes o vídeos.

Red.es (2015) nos explica que en la adolescencia la necesidad de autoafirmación, de pertenencia a un grupo o de definición sexual, motiva a los jóvenes para seguir realizando estas prácticas, añadiendo las siguientes motivaciones en la práctica:

- Presión de los demás, por ejemplo de la persona que les gusta.
- Para reforzar su autoestima y reafirmarse.
- El desconocimiento de las consecuencias hace verlo como conduzca sin riesgo.
- El contexto cultural de los menores influyen en la normalidad del fenómeno, del

mismo modo que podría verse como una aberración.

- Etc.

Entre los jóvenes es habitual, como veremos en la investigación, que dispongan de Smartphone propio, lo que facilita esta práctica. En ocasiones, los jóvenes hacen fotos o vídeos de sí mismos en situaciones íntimas ya se para enviárselos a otras personas o por simple curiosidad. El problema reside en que en ocasiones los teléfonos móviles son extraviados, olvidados en algún lugar o prestados a terceras personas. Esta situación pone en riesgo al joven, por lo que no es recomendable guardar información privada, que pueda dañarnos, en un dispositivo del que podemos perder el control.

Situación de la exposición al riesgo

INTECO (2011) nos dice que el 4,3%, de los menores participantes en el estudio realizado, ha recibido imágenes sugerentes de personas de su entorno (sexting pasivo) y un 1,5% reconoce haberse hecho a sí mismo fotos de carácter sexy (sexting activo), siendo las chicas las que más practican el sexting activo (2,2% frente al 0,9% de los chicos). En cambio, el sexting pasivo es practicado mayormente por los chicos (5,1% frente al 3,3% de las chicas).

Por su parte, Protégeles (2014), más preciso en la variable de la edad, obtiene que el 4,1% de los niños de 11 y 12 años de edad han recibido mensajes de contenido sexual y el 0,8% lo han enviado, mientras que el 13,7% de los jóvenes de 13 y 14 años los han recibido y el 2,4% lo has enviado. En el último caso se observa que se triplica el número de jóvenes que han enviado imágenes sexuales de sí mismos.

El estudio online “Sexting, una amenaza desconocida” (2012) desarrollada, en

América latina, en colaboración entre las iniciativas PantallasAmigas, eCGlobal Solutions, eCMetrics y CLIPS en la que participaron cerca de 5500 personas mayores de 18 años, revela que el 40% de los internautas han practicado Sexting en alguna ocasión.

Se observa, por tanto, que las variables de género y edad, son especialmente significativas en el estudio del sexting.

#Aftersex

Últimamente se ha extendido una moda que tiene cierta relación con el sexting llamada #aftersex que consiste en enviar imágenes, generalmente, aunque también pudiera tratarse de un vídeo, en el que aparezca una persona o una pareja, como indica su propio nombre "después del sexo", después de haber mantenido relaciones sexuales.

Lo más común consiste en enviar un tweet con el hashtag #aftersex en el que aparece la persona después de haber mantenido relaciones sexuales con tu pareja con cara de felicidad o entre sábanas. Es necesario tener en cuenta que cualquier usuario de Twitter puede acceder a la información enviada con ese hangstag.

Esta nueva iniciativa pudiera desencadenar ciberbullying, llamar la atención de depredadores sexuales y afectar su reputación e identidad digital.

Consecuencias del sexting

La sextorsión, ciberbullying, pornografía infantil y daños al honor, intimidad e imagen son los principales problemas que se pueden derivar de esta práctica (PantallasAmigas).

Otras consecuencias son (Red.es, 2015e):

- Humillación y linchamiento social, que puede acarrear una insoportable presión psicológica y social.
- En ocasiones las víctimas no lo hablan con sus padres, lo que les hace sentirse solos e indefensos.
- Pérdida de confianza en las relaciones con iguales, aislamiento, sentimiento de vulnerabilidad, etc.
- Las anteriores consecuencias producen depresión, ansiedad, tristeza, etc. Llegando en los casos más extremos incluso al suicidio.
- Estás consecuencias pueden desencadenar ciberbullying y en algunos casos sextorsión.

La existencia de contenidos eróticos vinculados a un menor le pone en riesgo de posibles devoradores sexuales que ven en estos contenidos el modo de coaccionarlo para conseguir sus propósitos. De ésta situación vamos a hablar a continuación.

e) Sextorsión

En la definición obtenida de la Wikipedia y difundida por PantallasAmigas, la sextorsión es una forma de explotación sexual en la cual una persona es chantajeada con una imagen o vídeo de sí misma desnuda o realizando actos sexuales que, generalmente, ha sido previamente compartida mediante "sexting". La víctima es coaccionada para tener relaciones sexuales con alguien, entregar más imágenes eróticas o pornográficas, dinero o alguna otra contrapartida, bajo la amenaza de difundir las imágenes originales si no accede a las exigencias del chantajista. (Wikipedia, 2013)

La sextorsión puede ser realizada por iguales, o bien, de adultos a menores lo que convertiría al suceso en un acto de cibergrooming con sus mismas consecuencias.

En caso de darse entre iguales, las consecuencias sufridas por las víctimas, además de las mencionadas habría que incluir las derivadas del sexting

Prevención Sexting y Sextorsión

La mejor prevención es inculcar a nuestros jóvenes la cultura de la privacidad. Es necesario hablar con ellos sobre los riesgos y consecuencias que puede desencadenar el envío o la publicación de información de este tipo. Por otro lado hay estudios que demuestran que el sexting se quintuplica entre los adolescentes que se pagan ellos mismos las facturas del móvil. Es importante, además, trasmitir y fomentar confianza con los jóvenes para que en caso de verse en una incidencia en la red acudan a un adulto (Colaboración Inteco - PantallasAmigas, 2011).

Red.es (2015) algunas proporciona recomendaciones para transmitir a los menores:

- Informar de los riesgos y consecuencias del envío y publicación de contenidos sexuales.
- Inspirar confianza a los jóvenes para favorecer la comunicación con los menores quien deben confiar en sus padres como las personas de referencia si experimentan alguna experiencia desagradable en la red.
- Fomentar la cultura de la privacidad.
- Ser conscientes que no existe sexting seguro, del mismo modo que no es seguro

disponer en mi teléfono personal de contenidos sexuales de mí o mi pareja.

- Se debe tener instalado software antivirus y bloquear el Smartphone con contraseña, para evita que alguien pueda entrar en nuestro dispositivo.
- Transmitir que los actos tienen consecuencias y que la legislación española actúa contra las personas que cometen delitos cibernéticos como la sextorsión.
- Valorar adecuadamente la imagen digital, la información que se comparte y a ser posible que en las imágenes que se reenvíen no aparezca el menor.

Otros consejos (Colaboración Inteco - PantallasAmigas, 2011):

- Conocer el nivel de seguridad y privacidad de los dispositivos y aplicarlo de manera responsable.
- No ceder ante la presión ni el chantaje
- No ser partícipe del sexting: ni creándolo, ni reenviándolo, ni fomentándolo.

f) Vulneración de derechos de propiedad intelectual

Según los resultados obtenidos por Inteco (2009) cerca del 50% de los menores y padres de menores son conscientes de la existencia de prácticas contra la propiedad intelectual (descargas ilegales de música, películas, juegos, software, etc.) y el 39,7% de los menores encuestados afirma realizar descargas de películas, juegos o programas sin licencia. "Moderado nivel de conocimiento, baja gravedad percibida y elevada incidencia declarada son los ingredientes de lo que se posiciona como una práctica habitual".

Esto demuestra escasa sensibilización sobre las consecuencias derivadas de la vulneración de los derechos de la propiedad intelectual, así como de las consecuencias

que podrían existir contra el menor. Es necesario difundir el conocimiento de las leyes que defienden los derechos de la propiedad intelectual y sus efectos sobre la sociedad y sobre la persona.

Consecuencias

Actualmente existe una gran preocupación por parte de las autoridades legales para proteger los derechos de propiedad intelectual, quien siguiendo recomendaciones de la Comisión Europea considerar imprescindible adaptar las leyes de España a la realidad que exige la Sociedad de la Información.

La respuesta no se ha hecho esperar y tras la polémica "Ley Sinde", seguida por la "Ley Lasalle" de 2013, el 4 de noviembre de 2014 se modificó la ley de Propiedad Intelectual en España y el 31 de marzo la modificación del código penal en éste ámbito.

Los abogados Andrea Luque y José Sánchez de León (2015), nos informan de los cambios que concentra la ley que nos ayudará a analizar sus principales modificaciones en cuanto al 'Fortalecimiento de los instrumentos para la lucha contra la vulneración de los derechos de propiedad intelectual, especialmente en Internet':

- Identificar a presentadores de servicios cuando esté infringiendo derechos con la propiedad intelectual o industrial.
- Perseguir a las webs que faciliten enlaces a contenidos ilícitos y elevar la cuantía a imponer. Para su identificación se podrá colaborar con los prestadores de servicios de la sociedad de la información que presten servicios a los infractores.
- Se introduce la figura extranjera de la *indirect liability*, en español

responsabilidad indirecta, de manera que podrán ser responsables de derechos quienes induzcan a la infracción o cooperen con ella. De su aplicación quedan excluidas las conductas marginales de particulares.

El 31 de marzo de 2015, se publicó la Ley Orgánica 1/2015, por la que se modifica el Código Penal, que ha introducido importantes cambios al régimen de los delitos contra la Propiedad Intelectual e Industrial que el abogado José Sánchez de León (2015) nos detalla:

- Se amplían las conductas que pueden constituir delito contra la Propiedad Intelectual.
    - Reproducir, plagiar o comunicar obras sin autorización, u obtener beneficio económico de su explotación.
    - Facilitar enlaces a contenidos protegidos sin autorización de los titulares. Esta disposición persigue la criminalización de la actividad de las llamadas 'web de enlaces'.
    - Facilitar información sobre saltarse filtros de seguridad o cualquier medida tecnológica de protección de los contenidos.
- Se extiende el significado de ánimo de lucro, en las acciones en las que se puede constituir delito contra la Propiedad intelectual, incluyendo cualquier beneficio directo o indirecto.
- Se incrementan todas las penas en los delitos contra la Propiedad Intelectual.

Podemos ver más información sobre todas las leyes que deben conocer los usuarios de Internet en el apartado de "Leyes y normativas españolas relativas a la seguridad en Internet".

Situación de la exposición al riesgo

En 2012 la policía nacional detuvo a 270 personas por delitos contra la propiedad intelectual, y en 2011 a 317 (EFE, 2013). La persecución por el momento no atañe a los consumidores de "piratería", aunque no es incoherente pensar que es cuestión de tiempo que esto ocurra. Es por ello, que se hace necesario que los internautas conozcan las leyes de propiedad intelectual, ya que el desconocimiento de alguna de ellas no exime de su cumplimiento, tal como dice el código civil en su artículo 6.

En el estudio de Minetur (2014) los padres afirman que "permiten a sus hijos/as, sin comprar, descargar contenidos (música y películas) en Internet".

Prevención

El Observatorio Europeo de las Vulneraciones de los Derechos de Propiedad Intelectual (2013) establece la sensibilización de la opinión pública como uno de sus pilares principales. El plan de trabajo pretende mejorar la comprensión de los problemas relativos a la propiedad intelectual mediante la muestra de aportaciones de la PI al crecimiento y al empleo en la UE y consecuencias de no respetarla.

El software de control parental permite restringir el acceso a páginas de descarga de archivos, así como el uso de programas de intercambio de información, lo cual, puede ayudar a prevenir conductas indeseadas de los adolescentes (INTECO, 2008).

Anteriormente, hemos visto otro de los riesgos de los que se ha hablado en esta investigación es la utilización y uso de manera incorrecta que hacen los menores de materiales con derechos de autor.

Hasta no hace mucho, Internet ha funcionado de manera anárquica en España, donde la industria era una de los principales perjudicados. El desarrollo económico vinculado a las tecnologías de la información y la comunicación no podría potenciarse sin la ayuda de un sistema jurídico que proteja sus intereses.

El empoderamiento de los jóvenes en el ámbito tecnológico se antoja imprescindible al ser ellos mismos quien constantemente toman decisiones sobre sus acciones en Internet y por lo tanto ser responsables de ellas. Los jóvenes deben conocer las leyes establecidas en el ámbito digital del mismo modo que necesitan conocer las que les rodean en su vida off line.

Es necesario que la industria, por su parte, facilite toda la información posible en cada momento de los materiales disponibles en la red y desarrollar nuevos formatos de información que permita a los jóvenes entender las repercusiones legales de lo que hacen en la red.

Todos los usuarios de las tecnologías de la información y la comunicación y, más concretamente de Internet, conozcan la repercusión de sus acciones en cuanto a materiales digitales con derechos de autor se refiere. En este sentido, las autoridades competentes tienen el deber de realizar campañas de sensibilización e información sobre las modificaciones y adaptaciones de las leyes que poco a poco están legislando todas las acciones de Internet, dado que partimos de haber creado unos hábitos en un entorno digital sin legislar en el que todo ha estado permitido.

g) Acceso a contenidos inapropiados

Una de las principales ventajas que ofrece el acceso a la red es el acceso a todo

tipo de contenidos. Ésta, a la vez, es uno de sus principales y más frecuentes riesgos si se trata de un menor.

La red está formada por millones de páginas web que nos ofrecen bienes, servicios o simplemente ponen información a disposición del internauta. Las páginas web pueden ser creadas por empresas con fines comerciales, por internautas con afán de compartir información, de crear espacios para personas con unos mismos intereses, por personas que persiguen algún tipo de beneficio, etc. Sin embargo, los contenidos expuestos no siempre tienen un control legítimo que garantice su fiabilidad, dando lugar a páginas web con dudosos contenidos, contenidos ilícitos u otros contenidos nocivos que puedan resultar perjudiciales para los jóvenes. Se puede decir que los jóvenes tienen a un solo 'clic' multitud de contenidos inapropiados, entendiendo por inapropiados todos los materiales existentes que puedan resultar dañinos para el menor.

Sea información, imágenes, audios o vídeos los contenidos nocivos pueden ocasionar graves perjuicios en el desarrollo de niños y adolescentes, a través de páginas web con imágenes, actitudes, comportamientos o valores negativos (Red.es, 2015a).

Algunos de los contenidos considerados más perjudiciales para los jóvenes son los siguientes (Red.es, 2015a):

- Contenido de carácter sexual inapropiado o pornográficos: son contenidos inadecuados a la edad de los menores por falta de capacidad de asimilación de lo que están viendo. Ofrecen una visión distorsionada de las relaciones sexuales, de la sexualidad pudiendo generar obsesión.
- Violencia, racismo o contenidos sexistas: imágenes y vídeos de palizas, torturas, vejatorios con personas por su identidad sexual, raza, ideología, religión, o de

maltrato animal o destrozo del mobiliario urbano. Estos contenidos pueden ser expuestos con la intención de hacer apología de estos actos e incitar a los cibernautas a hacer algo similar. En ocasiones, les acompañan foros o chats donde los autores, u otros internautas muestran su apoyo a estos comportamientos y defienden las conductas violentas. Los videojuegos o juegos on line, también pueden recrear este tipo de violencia, debiendo el jugador de realizar violaciones, asesinatos, etc., para superar la fase (Bottero, Escoto y Goncálvez, 2006).

- Anorexia, bulimia o cuestiones estéticas perjudiciales: Es común encontrar ideales de belleza en medios TIC que realza los ideales de belleza. Esto ha dado lugar a graves conductas que poner en riesgo la salud física y psicológica. Un ejemplo de ello, son las técnicas de blanqueamientos dentales fomentadas que pueden llegar a causar la muerte del diente, o las páginas pro-anorexia y pro-bulimia, proANA y proMIA respectivamente, de las cuales vamos a hablar en otro apartado debido a la gravedad del daño que pudiera causar la exposición al riesgo y el incremento que ha habido en los últimos años como veremos a lo largo de la investigación.
- Sectas o terrorismo: hace pocos meses la Casa Blanca advertía sobre el aumento del uso de las redes sociales por parte de yihadistas en busca de mujeres, niños y jóvenes. En Brasil están preocupados por informes que han recibido en los que se buscan jóvenes a través de las RRSS por el Estado Islámico (Voz de América, 2015). A raíz de éstos informes el país ha elevado la alerta terrorista de cara a los juegos de 2016 (El País, 2015)

- Contenidos falso, inexacto o incierto: puede tratarse simplemente de contenidos falso por error o desconocimientos del creador, o bien, leyendas urbanas que supuestamente han ocurrido y que se propagan rápidamente por la red por las historias extravagantes que propagan. También puede tratarse de mensajes en cadena que pretenda crear alerta, engañar al emisor o solicitar datos personales para usarlos de forma fraudulenta o maliciosa (Gómez, 2011).
- Vídeos virales: Se tratan de grabaciones de jóvenes realizando alguna práctica que en ocasiones puede resultar altamente peligrosa. Un ejemplo es el de introducir alcohol en los ojos para conseguir un efecto inmediato del alcohol. Se propagan a través de redes sociales, mensajería instantánea, correo electrónico, etc.
- Contenidos de juegos y apuestas: la industria de los juegos de azar está creciendo exponencialmente en los últimos años, siendo su principal riesgo la apariencia inofensiva que presenta. Es necesario hablar con los jóvenes sobre este tipo de ocio.

Los contenidos expuestos son considerados nocivos por los motivos argumentados, sin embargo, ello no significa que sean ilícitos. Algunos tales como la pornografía infantil, la apología del terrorismo, el racismo o el tráfico de drogas están perseguidos por la ley, aunque bien es cierto que hay multitud de contenidos legales que pueden resultar nocivos para el joven. (INTECO, 2009, pág. 77).

Situación de la exposición al riesgo

En el estudio de Minetur (2014) el 26% de los jóvenes dice haber visto algo que le ha molestado por Internet, con una frecuencia inferior a dos veces al mes el 54% de

los casos. El 35% de los jóvenes de 17 años afirman haber visto contenidos que les han molestado, con una frecuencia de una o dos veces al mes en el 30% de los casos.

Garmendia et al. (2011), en el estudio elaborado con menores de 9 a 16 años, encontraron que los contenidos inapropiados y potencialmente peligrosos para los menores más visitados son los contenidos sobre odio contra otros grupos o personas (11%), las páginas web que promueven los desórdenes alimenticios (7% y 12% en el caso de jóvenes de 15 y 16 años), las que hablan de experiencias consumiendo algún tipo de droga (7%) y las que promueven la autolesión (6%).

Los padres muestran una creciente preocupación por la exposición a contenidos inapropiados a la edad de sus hijos. Al 65% les preocupa que accedan a imágenes explícitas de sexo o violencia, cerca del 60% les preocupa que sean víctimas de cibergrooming y al 55% que accedan a información dañina para su edad (Hasebrink, Olafsson, & Stetka, 2009).

Según McAfee (2012) siete de cada diez jóvenes de entre 13 y 17 años ocultan sus actividades en Internet. Por otra parte solo el 12% de los padres creen que sus hijos adolescentes ven pornografía en línea.

Comunidades peligrosas on line

Las comunidades on line son grupos de personas con intereses común que interactúan en un mismo espacio virtual. En éstos lugares pueden adquirir una identidad digital, lo que les permite ser reconocidas dentro de la comunidad por su actividad, pero no off line. Puede darse que lo jóvenes busquen en éstas comunidades el reconocimiento y comprensión que no encuentran en su vida off line.

Dependiendo de los intereses de la comunidad, las prácticas y objetivos de la comunidad pueden resultar realmente nocivos para los menores. Las principales comunidades peligrosas son (Red.es, 2015b, págs. 4-8):

- Comunidades pro-anorexia y pro-bulimia. Debido al gran riesgo que representan para sus usuarios y al incremente que han tenido en los últimos años hablaremos de este riesgo más detenidamente a continuación.
- Comunidades que fomentan la autolesión.
- Comunidades que fomentan el odio "hate-speech". El ámbito es el odio basado en la intolerancia ya sea por motivos ideológicos, sexista, raza, cultura, religión, etc.
- Comunidades que promueven hábitos de vida no saludables como el consumo de alcohol y drogas.
- Comunidades que realizan apología del suicidio.
- Comunidades que realizan apología de la pedofilia.
- Comunidades relacionadas con juegos on line.

Estas comunidades están presentes en foros, blogs, redes sociales, etc. El problema de su seguimiento es que se una vez está establecida la comunidad puede cambiar el medio de contacto a la mensajería instantánea lo que dificulta su seguimiento.

Comunidades pro-anorexia y pro-bulimia

Desde hace más de 10 años las páginas web proANA y proMIA han preocupado a todas las autoridades competentes, quienes han realizado diversas acciones para evitar que se propaguen por Internet y adquieran seguidores y seguidoras que accedan a ellas

buscando “comprensión y refugio” en comunidades cibernéticas de personas con trastorno de la conducta alimentaria.

ANA y MIA, es la personalización que le han dado a las páginas web que fomentan y hacen apología de la anorexia y la bulimia. Así, se han instaurado en Internet miles de páginas y denominadas proANA y proMIA, o lo que es lo mismo, pro-anorexia y pro-bulimia.

No se han establecidos las causas que provocan la anorexia nerviosa, sin embargo, la comunidad médica ha consensuado que las causas no son biológicas sino que se deben a factores ambientales y del entorno de los individuos, como: la presión social, los cánones de belleza, etc. Siendo el entorno y, más concretamente en la red, dónde se crean las páginas web pro-ANA y pro-MIA (Protégeles, 2005, pág. 23).

Figura 2 Princesa Lorelei ProANA *(Princesa Lorelei, 2015)*

Protégeles, bajo encargo del Defensor del Menor, realizó un estudio en el año 2005 llamado ‘La prevención de la anorexia y la bulimia en Internet’ en el que advierte de la peligrosidad de las páginas web proANA y proMIA. En el estudio, aporta un listado de páginas web que consiguieron cerrar recientemente al estudio, por hacer

apología a la red de la anorexia y/o la bulimia para luchar contra la proliferación de estas páginas.

Protégeles se ha implicado en la lucha contra este tipo de páginas denunciando a cientos de ellas para que sean cerradas y, de éste modo, los y las jóvenes al perder el contacto con los grupo pro-bulimia y pro-anorexia se acerquen a programas de recuperación (Protégeles, 2005, pág. 85)

¿Qué información contienen las páginas web proMIA y proANA para ser consideradas altamente peligrosas y nocivas para los y las jóvenes?

Cualquiera que disponga de un dispositivo con conexión a Internet puede acceder a alguna de las cientos de páginas que existen proMIA y proANA. En ellas te explican que ser proANA y/o proMIA es un estilo de vida. Una forma de enfrentarte a la vida con orgullo, con fuerza y con valentía, que te permitirá afrontar grandes retos para conseguir tus propósitos y con ello ser más feliz.

Antes de entrar al contenido de las páginas nos encontramos que en algunas de ellas te animan a participar en los desafíos que proponen para adelgazar e instan a los y las usuarias que no estén de acuerdo con el contenido a salir de la página. Una vez dentro, promueven que el lector o la lectora se sienta especial y valiente por perseguir sus objetivos, incluso les animan a identificarse portando pulseras o algún tipo de distintivo que muestren orgullosamente según el tipo de retos que estén dispuestas a aceptar. Explican diversos métodos de adelgazamiento, o formas de vencer al hambre, instaurando el término de ‘fracaso’ si no cumples con tus objetivos o castigos que consisten en auto infligirse dolor “self injury”.

Te proponen castigos como hacerse cortes en la piel cuando piensas en comida, con la intención de purgar "tu pecado" y no caer en la tentación de comer. Se convierte en una fuente de desinformación, llena de falsos mitos altamente peligrosos para la salud (Agència de Qualitat d'Internet en colaboración con la Associació contra l'Anorèxia i la Bulimia, 2010, pág. 5). Incluso proponen fármacos o componente químicos que contienen algunos fármacos para adelgazar. Algunos de ellos han sido causantes de la muerte de muchas personas, cómo la sibutramina, en España comercializada con el nombre de Reductil y que en Estados Unidos fue retirada después que muriesen 32 personas que la consumían (Agència de Qualitat d'Internet en colaboración con la Associació contra l'Anorèxia i la Bulimia, 2010, pág. 3).

Figura 3 Imágenes ProANA y ProMIA

Fuente: Agència de Qualitat d'Internet en colaboración con la Associació contra l'Anorèxia i la Bulimia. (2010).

Las páginas proANA y proMIA, fomentan la pertenencia al grupo, realzan la valoración de la estética sobre la salud, defienden la bulimia y la anorexia como un estilo de vida válido sólo apto para las personas valientes y luchadoras, animándose

unas a otras a perseguir sus objetivos haciendo frente a cualquier obstáculo que se interponga en su camino.

Es evidente el peligro que representan para las personas con trastorno de la conducta alimenticia o para todas aquellas personas que sean sensibles a desarrollarlo.

¿En qué tipo de páginas se hace apología de la anorexia y la bulimia?

En el informe "Las páginas "pro ana" y "pro mia" inundan la red"creado por IQUA y la Asociación española contra la anorexia y la bulimia, nos explican que, en España, las páginas Inicialmente fueron creadas por usuarios con el objetivo común de adelgazar en espacio virtuales como spaces.live.com y groups MSN. Posteriormente, IQUA detectó que la mayoría de páginas y espacios con estos contenidos son páginas personales y blogs, alojadas en plataformas reconocidas a nivel mundial como Google e Hispavista que, a su criterio debería asumir cierta responsabilidad e impedir la apertura de páginas con este tipo de información.

También encontramos información sobre apología de la anorexia y la bulimia en foros donde los participantes pueden intercambiar opiniones y aportar información que en ocasiones obtienen de otras páginas web proANA y proMIA.

Podemos observar también en el caso de los foros que no se ocultan, si no lo contrario, son explícitos sobre la información que contienen.

En el informe mencionado, te ofrecen foros y páginas de ayuda a la recuperación de personas con trastornos de la conducta alimenticia donde explican que los comentarios están controlados por moderadores, como www.foroanaymia.com. Sin embargo, a día de hoy la página ya no contiene este tipo de información. Si tenemos

disponibles otros hilos en foros que han ido surgiendo como es el caso de http://foro.enfemenino.com/forum/psycho1/__f8067_psycho1-Grupo-de-recuperacion-para-anorexia-bulimia.html. En él se pueden encontrar comentarios de niños y niñas, que abren su corazón y explican el "infierno" que están viviendo y del que desean salir pero son incapaces.

También encontramos grupos y comunidades creados en redes sociales que fomentan estas conductas donde sus participantes muestran opiniones a favor y otras veces en contra y que, en ocasiones, queda más claro y revelador el mensaje de la persona que es capaz de exponer mejor sus ideas, sea una voz en contra de la anorexia y la bulimia o a favor de ellas.

Otro medio en auge es la mensajería instantánea como WhatsApp o Link que facilitan la creación de grupos de personas afines. Este caso es más difícil de rastrear al ser un medio "privado" que sólo pueden acceder a él las personas agregadas o invitadas.

¿Quién crea las páginas web proANA y proMIA?

Lo más habitual es que las administradoras y/o creadoras del espacio web sean personas que sufren algún tipo de trastorno de la conducta alimentaria, quienes están en situación de riesgo de padecerlo o que han participado en alguna de las actividades o experiencias de éstas páginas (Fundación imagen y autoestima, 2013).

¿Qué hacer al detectar una página que hace apología de trastornos de la conducta alimentaria?

La Fundación Imagen y Autoestima propone en su página web denunciarla a través de la Asociación contra la anorexia y la bulimia, activándose el protocolo mostrado en la Figura 4.

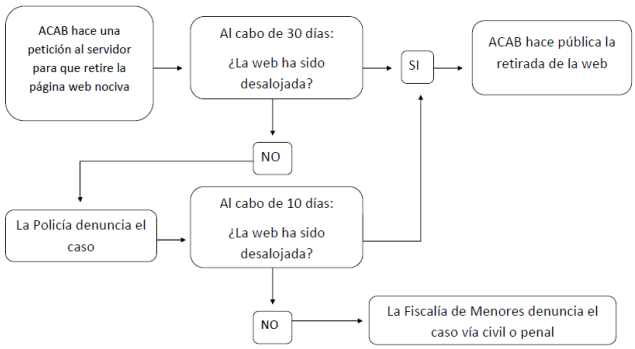


Figura 4 Protocolo denuncia *(Fundacion imagen y autoestima, 2013)*

Además, en la página de la Fundación existe un formulario para denunciar a las páginas web que hacen apología de la anorexia y la bulimia.

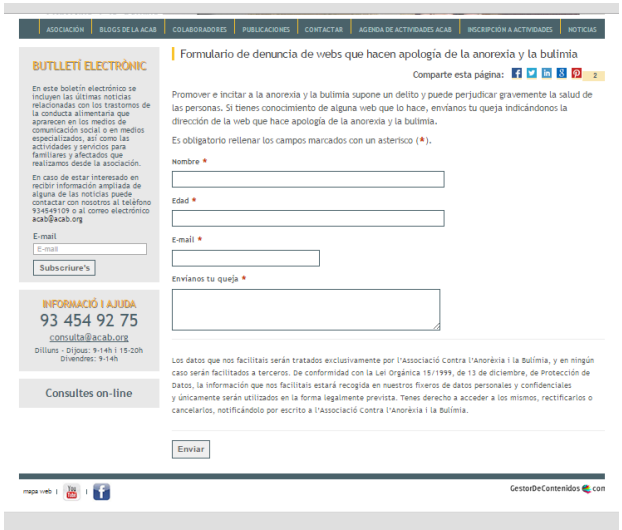


Figura 5 Formulario de denuncia apología de la anorexia y la bulimia (Asociación Contra la Anorexia y la Bulimia de Cataluña, 2015)

EU Kids Online, constata que en 2010 las consultas de los y las jóvenes un 9% que han consultado páginas que hacen apología de la anorexia y la bulimia y en el año 2014 ha aumentado hasta un 13% (EU Kids online, 2014). El estudio fue realizado en 7 países: Bélgica, Portugal, Dinamarca, Italia, Irlanda, Rumanía y Reino Unido. Aunque España no forma parte de los países en los que se llevó a cabo la investigación nos permite entender la gravedad de la situación y obtener ciertas conclusiones sobre la efectividad de las medidas realizadas para paliar los efectos nocivos del uso de las TIC en cuanto al acceso de éste tipo de contenido inapropiado y de la situación de vulnerabilidad que viven los y las jóvenes.

Sin menospreciar el mérito de la eliminación de páginas webs proMIA y proANA que se ha realizado en la última década, la facilidad para crear páginas web informativas, hilos de conversación en foros o chats y la dificultad de su localización, hace que la denuncia pueda resultar insuficiente y sea necesario implementar otros métodos para evitar la proliferación de éste tipo de páginas web. La Agència de Qualitat d'Internet (Iqua) denunció que entre el 2006 y el 2008 las páginas web proMIA y proANA aumentaron un 475% por encima del porcentaje de crecimiento de gigantes como Facebook o Myspace (Estirado, 2015).

Son muchas las personas que les preocupa especialmente que los y las jóvenes tengan a su disposición páginas proANA y proMIA debido al gran peligro que representan las enfermedades de la conducta alimentaria, por lo que actualmente se están recogiendo firmas a través de Change.org para que se prohíba su creación, contando con más de 250000 firmas por el momento. (Visita a Change.org realizada el 7 del 7 de 2015)

Se puede observar que la dirección web de las páginas aporta información sobre su contenido e incluso de la aceptación que las personas que la visitan tienen sobre las enfermedades relacionadas con la conducta alimentaria. Es evidente que no quieren ocultarlas. No quieren ocultar sus objetivos, ni sus creencias. Incluso, podemos afirmar que lo que ocurre es lo contrario. Están orgullosas de formar parte de este grupo, de ser proANA y proMIA. Quieren ser Ana o Mia. A nosotros nos aterran las consecuencias que pueden desencadenar éstos hábitos de vida, sin embargo, en éstas páginas todo lo contrario a avergonzarse de lo que viven, muestran con orgullo lo que denominan su "estilo de vida".

Como hemos visto, son muchas las páginas que se han conseguido cerrar gracias a iniciativas internacionales y nacionales temerosas de los efectos nocivos de las páginas proANA y proMIA, desde hace más de 10 años. Lamentablemente, hoy se puede afirmar que las medidas tomadas no son suficientes, ya que lejos de bajar el número de jóvenes que acceden a éstas páginas se ha aumentado notablemente. Ello, nos hace plantearnos nuevas o viejas preguntas, según se mire: ¿estamos tomando el camino correcto para paliar las consecuencias nocivas derivadas del uso de las TIC?, ¿es la prohibición la solución?, ¿tenemos otras soluciones o es que se trata de la solución más fácil de implementar?, ¿es posible controlar el acceso a las páginas con contenidos inapropiados?, ¿es la información la culpable de las conductas?

Prevención

Una medida práctica para evitar que los menores accedan a páginas web, voluntaria o involuntariamente, con contenidos inadecuados a su edad es instalar software de control parental. El software de control parental nos permite,

principalmente, filtrar aquellas páginas web que contengan las palabras claves seleccionadas en el filtro, limitando así el contenido de las páginas a las que se puede acceder. Este tipo de recurso no ofrece protección total, sino que debe ser utilizado con otras técnicas como la supervisión y la sensibilización que permita a nuestros hijos ser protagonistas de su proceso madurativo (Madrid Salud - Instituto de adicciones). Sin embargo, estas medidas no han demostrado una menor exposición de los jóvenes adolescentes a los riesgos (Mascheroni & Cuman, 2014), aunque si puede resultar útil en el caso de los menores más pequeños.

EU Kids Online (2011), financiada al amparo del Programa Safer Internet de la UE, realizó un estudio a 26 programas de control parental en el que obtuvo que el 84% de los programas informáticos de control parental probados permiten a los padres bloquear el acceso a determinados sitios de Internet, aunque son menos eficaces en filtrar contenidos de la Web 2.0, tales como las redes sociales o los blogs. Además, solo unos pocos productos del mercado son capaces de filtrar los contenidos de Internet a los que se puede acceder a través de los teléfonos móviles o las consolas de videojuegos.

Existen buscadores diseñados para los menores de edad que sólo muestran resultados de contenidos seguros parar ellos. Algunos ejemplos son yahoo! Kids, Ask Kids o configurar los buscadores habituales como google, yahoo, bing, etc. en la opción de búsqueda segura.

También es necesario que se conozcan las aplicaciones adecuadas para los menores para darles alternativas a la restricción. Un ejemplo de ello es Youtube Kids como alternativa a Youtube.

En el caso de los adolescentes, gracias a la facilidad de acceso a Internet, en parte debido a los Smartphones, si quieren acceder a determinados contenidos muy posiblemente encontrarán el modo de hacerlo. El camino parece estar más orientado a la educación y sensibilización sobre los riesgos existentes en el acceso a contenidos inapropiados, fomentando un uso responsable y seguro de las mismas, buscar alternativas a la restricción ya que puede aumentar el deseo de acceso, compartir tiempo de navegación con los jóvenes, etc. En el caso de contenidos ilícitos se pueden denunciar con el objetivo del cierre de la página. A lo largo del informe veremos que es el camino que se está siguiendo en estos casos para la defensa y protección del menor, aunque esta restricción de acceso a la información en ocasiones puede crear controversia.

El papel de padres y educadores resulta fundamental en la relación del joven en el uso de las TIC.

En los últimos años se ha fomentado la catalogación de los contenidos digitales, entre los que podemos destacar los siguientes sistemas de clasificación (Red.es, 2015a, pág. 19):

Criterios del instituto de cinematografía y de las artes audiovisuales (ICAA): establece criterios para poder calificar por grupos de edad los contenidos audiovisuales y su exhibición.

Clasificación PEGI y PEGI on line: creado para ayudar a los padres a conocer la edad recomendada en los videojuegos.

h) Amenazas a la privacidad

La privacidad en Internet es el control que tiene un usuario de Internet sobre su información personal cuando interactúa con alguno de los servicios on line con los que intercambia datos durante la navegación (Red.es, 2015c).

La privacidad de nuestra información es uno de los riesgos que más repercusión puede tener para nuestra seguridad, cuya vulneración constituye un delito (Pantallas Amigas, 2011).

En la red es necesario que todos los usuarios realicemos una buena gestión de la privacidad con el fin de evitar algunos de los riesgos derivados del uso de las TIC que hemos mencionado y estafas, ya que nuestra información personal puede ser utilizada de forma fraudulenta.

Cuando nos referimos en Internet a información personal nos referimos a cualquier información sobre nuestra persona, como pueden ser datos personales identificables de la persona pero también información sobre nuestros gustos, forma de ocio, aficiones y por supuesto imágenes, vídeos o audios.

Características de la privacidad on line (Red.es, 2015c):

Debemos tener en cuenta que la información que una persona sube a la red jamás volverá a ser privada. Es decir, una vez subida no se volverá a tener el control sobre dicha información. Si se desea que desaparezca, se podría eliminar pero el borrado no garantiza que vuelva a aparecer en la red, dado que cualquier persona que haya tenido acceso a la información podría haberla descargado y si quisiera podría difundirla a otras personas.

Del mismo modo que en nuestra vida off line tenemos y vivimos con pautas de privacidad que hemos aprendido y utilizado desde pequeños, es necesario utilizar pautas de seguridad y privacidad en nuestra vida on line. El valor de la privacidad on line debe ser trasmitido a los menores, por familias y educadores, de tal modo que comprendan las consecuencias que tienen sus decisiones en la web.

Especialmente los menores tienden a sentir la necesidad de tener reconocimiento social, aceptación y pertenencia al grupo, lo que son aspectos claves en el desarrollo del autoconcepto y autoestima, y utilizan las TIC en busca de estos propósitos mediante su exposición en la red. Además, en la adolescencia tener "audiencia" que les reafirme y refuerce cobra gran importancia, lo que en ocasiones se traduce en permitir que gran número de personas accedan a su información a través de servicios de redes sociales u otros servicios similares.

Todas las decisiones que toman los jóvenes sobre la exposición de su información personal pueden acompañarles por el resto de su vida. Desde que nos conectamos por primera vez a Internet comenzamos a crear lo que se define por "Identidad Digital". Así, está conformada por toda la información que subimos a Internet, es nuestra imagen en la red. La identidad digital es el resultado de lo que publicamos en redes sociales, blogs, foros, vídeos de youtube, opiniones, etc.

La exposición de información en la red ha llegado al punto que los jóvenes tienen identidad digital antes de conectarse por primera vez a Internet. Desde que nacen son muchos los padres que suben fotos y videos a Internet y las comparten con sus contactos, en ocasiones incluso con desconocidos.

No debemos olvidar que, detrás de gran parte de los servicios de Internet, existe un entramado empresarial cuya base de su negocio está en los datos de los cibernautas. Así, la información y derechos sobre nuestra información que cedemos al firmar el consentimiento para poder disfrutar de una aplicación o un servicio, juega un papel fundamental en la privacidad de nuestra información. Desde la llegada del Smartphone uno de los derechos que se le cede a gran parte de las aplicaciones es el de acceder a la geolocalización del dispositivo, lo que le da información a la aplicación de dónde se encuentra la persona en un momento determinado del día.

En este sentido, la Agencia Española de Protección de Datos (AEPD) ha participado en un análisis para examinar las condiciones de privacidad de las aplicaciones móviles más populares organizado por la Red Global de Control de Privacidad (GPEN).

En los últimos años se ha potenciado la publicidad dirigida al público jóvenes a través de videojuegos, teléfono móvil, páginas web frecuentadas por menores, etc.“. En este sentido, existe gran preocupación de las familias y colectivos vinculados a la protección de los menores relacionada con el impacto que puede generar la publicidad sobre los jóvenes y por el exceso de comercialización de la infancia”.

La revelación de información privada de terceros puede constituir un atentado contra el derecho a la intimidad recogido en el artículo 197 del Código Penal sobre el descubrimiento y la revelación de secretos por el que el autor de la sustracción podría ser condenado a penas de prisión de 1 a 4 años y multa de 12 a 24 meses (Ribas, 2012). El joven no solo puede ser víctima de delitos de publicación de información privada

sino que, también, puede, consciente o inconscientemente, ser autor de delitos que vulneren el derecho a la intimidad de otra persona.

Situación de la exposición al riesgo

El colectivo más vulnerable, debido a la tendencia de compartir información, (opuesta a la conducta de los adultos de retener la información) es el de los adolescentes (INTECO, 2009, pág. 80). Según datos extraídos de Red.es (2015) el 14,3% de los adolescentes han compartido información personal con desconocidos. Garmendia et al. (2011) afirma que el 14% de los jóvenes tiene un perfil público en su red social, lo que significa que cualquier persona puede acceder a él.

Por último, decir que los riesgos asociados a una mala gestión de la privacidad son el cibergrooming, ciberbullying, fraudes o sexting, lo que podría desencadenar los riesgos y daños vistos en cada uno de los apartados correspondientes a estos riesgos.

Prevención

Jorge Flores Fernández, experto en el uso seguro de las TIC y director de PantallasAmigas, portal web creado para la promoción del uso seguro y saludable de las nuevas tecnologías y el fomento de la ciudadanía digital responsable en la infancia y la adolescencia, establece 6 recomendaciones para la protección de la privacidad de los adolescentes en las redes sociales:

- Conocer y configurar de manera detallada las opciones de privacidad. Es necesario que el usuario de redes sociales conozca la opciones de configuración de privacidad de su cuenta en las aplicaciones web que prestan estos servicios,

sin embargo, se considera aún más importante conocer las consecuencias de tener una mala configuración de privacidad.

- Identificar las funciones y los efectos de cada acción. Es importante conocer los efectos derivados de las acciones que se realizan en el uso de la red social, dado que estos efectos no tenidos en cuenta pueden ser nocivos para el usuario.
- Proteger los datos personales. Sensibilizar a los usuarios de la importancia que tienen los datos personales se antoja imprescindible para evitar riesgos y acciones que puedan surgir.
- Proteger personalmente los datos. El principal filtro que pasan nuestros datos personales somos nosotros mismos.
- Mantener una actitud proactiva en la defensa de los datos propios. La difusión de contenidos privados acerca de otras personas es una tendencia negligente e incluso temeraria. El usuario debe supervisar la información facilitada por terceros sobre uno mismo, informando a los demás sobre nuestro criterio al respecto y/o ejerciendo nuestro derecho a eliminarlos.
- Evaluar las actitudes y condiciones de privacidad de los contactos. Un contacto que pudiera ser considerado y respetuoso puede afectar de manera involuntaria nuestra privacidad con una configuración de seguridad o acción inadecuada.

Todo esto indica que las familias juegan un papel fundamental en la educación on line de los menores, siendo los principales responsables de aportarles la información y las pautas a seguir en el uso seguro y responsable de la red, que incluye la correcta gestión de la privacidad.

i) Amenazas técnicas, virus y fraudes

El uso de la red nos expone al ataque de virus u otros programas informáticos, malware, con fines maliciosos. Las consecuencias pueden ser inmediatas como la pérdida de información o la ralentización del sistema o, en otros casos, puede ocurrir que el Cracker, persona con propósitos malintencionados, se quede como observador en nuestra máquina para robarnos información sigilosamente. (INTECO, 2009, pág. 82)

Los primeros virus solían centrar su actividad en causar pérdidas de información y molestias a los usuarios, corrompiendo archivos, impidiendo el uso de determinados programas, obstaculizando el arranque del ordenador, etc. En la actualidad, los objetivos suelen estar centrados mayormente en obtener datos bancarios, información personal, fotografías, datos de acceso a cuentas de servicios de Internet, uso de webcam, etc. (Red.es, 2015d, pág. 16).

El Convenio de Budapest del Consejo de Europa sobre Ciberdelincuencia recoge en su artículo 8 el fraude informático. El fraude informático es una modalidad de fraude que utiliza los medios electrónicos o informáticos para la comisión del delito y que afecta potencialmente a cualquier usuario de Internet (INTECO, 2009, pág. 81).

Aunque a priori el fraude económico no afecta especialmente a los menores por su falta de capacidad adquisitiva, en este contexto los menores podrían ser víctimas de fraudes u otros actos de ciberdelincuencia a través de la red, o acceder a actividades dirigidas a mayores de edad que puede implicar la perdida de dinero como los juegos de azar o las apuestas (INTECO, 2009).

Situación de la exposición al riesgo

También hay que mencionar el spam como una de las molestias que más afectan a los usuarios de Internet. Cabe señalar que, mientras el spam afecta al 85% de los usuarios, el 60% de los ordenadores están infectados por algún malware, referidos a los programas maliciosos que son capaces de esquivar al software de seguridad para instalarse en nuestros ordenadores (Red.es, 2015d, pág. 17).

El desarrollo de malware dirigido a dispositivos que usan la plataforma Android ha aumentado notablemente. Entre Junio del 2010 y Enero del 2011 creció un 400%, sin embargo, aproximadamente 50% de los usuarios de teléfonos móviles no protegen su terminal. Otro dato a tener en cuenta en el uso de teléfonos móviles es que hay 15 veces más posibilidades de perder un dispositivo de este tipo que de perder un ordenador portátil (McAfee, 2012, pág. 6).

En los últimos años se ha extendido la creación de páginas falsas que suplantan la identidad de páginas web de confianza. Es conocido por Phising. Aprovechan que los usuarios acceden a las páginas web en las que poseen cuentas de acceso desde links proporcionados a través de otras páginas web, correo electrónico, o suministradas por el buscador, sin prestan atención a la dirección web de la página antes de introducir los datos de acceso. Una vez suministrados los datos de acceso a la página web falsa, el creador puede cambiar la contraseña y quedarse con la cuenta, acceder a la cuenta y descargarse la información personal, o acceder sin que el usuario tenga conocimiento de ello y espiarle hasta que decida cambiar la contraseña.

Del mismo modo que nadie nos puede asegurar que saliendo a la calle no

tengamos ningún percance ya sea un accidente, que nos atraquen, etc..., en Internet no es posible garantizar la seguridad total de un dispositivo con acceso a Internet frente a ataques externos. Sin embargo, si se lo podemos poner muy difícil a aquellas personas que lo intenten, realizando actualizaciones del sistema, teniendo software de seguridad actualizado que impida y/o dificulte efectuar el ataque, además de tener hábitos de uso seguros en el uso en la navegación por Internet (Alonso, 2011).

Precauciones

Las empresas de antivirus ofrecen en sus páginas web una serie de medidas recomendadas para protegerse de cualquier programa con intenciones maliciosas contra nuestro dispositivo de conexión a Internet. La empresa McAfee, desarrolladora de productos para la seguridad tecnológica, nos ofrece las siguientes recomendaciones (Informador, 2010):

Disponer de software de seguridad integral. El software de seguridad, como mínimo debe incluir: funcionalidades antivirus, un firewall bidireccional contra programas espía, contra fraude electrónico y de búsqueda segura. Adicionalmente, aunque recomendable es disponer de antispam, software de control parental, protección de redes inalámbricas y protección antirrobo.

Es necesario tener actualizado permanentemente el software de seguridad. Los programas dañinos para nuestro ordenador encuentran constantemente nuevas formas de atacarnos, por lo que es necesario realizar las actualizaciones que nos protejan frente a las nuevas amenazas.

Utilizar el correo electrónico con precaución. No se debe enviar información

privada a través de nuestro correo electrónico, abrir mensajes de personas desconocidas o descargar información de vínculos desconocidos.

Fraudes electrónicos. Utilizan correos electrónicos y sitios Web fraudulentos, disfrazados de empresas legítimas, para atraer a usuarios confiados para que revelen información de cuentas privadas o de inicio de sesión.

Sensibilizar y formar a todos los usuarios del ordenador han de tomar las mismas precauciones, ya que las acciones de uno pueden perjudicar a todos. Se recomienda situar el ordenador en un área común que facilite la interacción entre padres e hijos. En caso de utilizar software de control parental se deberá asegurar que el menor que hace uso del ordenador no pueda desactivarlo.

Las contraseñas han de ser seguras, incluyendo mayúsculas, minúsculas, números, símbolos, etc. Se recomienda no usar la misma contraseña para distintas cuentas.

Realizar búsquedas y compras con seguridad. La protección integral del equipo informático incorpora software que califica las páginas web como seguras o no seguras. Antes de comprar se deben conocer las políticas de privacidad y seguridad de la tienda en línea.

Las *copias de seguridad* nos ayudarán a recuperar la información en caso de pérdida.

Los programas de mensajería instantánea deben utilizarse con precaución. Es recomendable no usar información personal como puede ser nuestro nombre. Además, en ningún caso, se debe aceptar a extraños en los grupos de mensajería instantánea.

Según McAfee los jugadores en línea son el segundo blanco para atacar de los desarrolladores de malware, software malicioso que, con frecuencia, atacan con troyanos que roban contraseñas, por lo que debe asegurarse de tener activado el software de protección cuando hago uso de las plataformas de juego on line.

Los dispositivos móviles presentan un conjunto de precauciones añadidas (McAfee, 2012, págs. 7-18):

- Bloquear el dispositivo mediante código PIN o contraseña.
- Instalar solamente aplicaciones desarrolladas por fuentes de confianza.
- Crear copias de seguridad de la información almacenada.
- Actualizar en sistema. Las actualizaciones solucionan fallos de seguridad del sistema y mejoran nuestra experiencia en su uso.
- No piratear el dispositivo. Al piratear un dispositivo móvil se pueden abrir brechas de seguridad o debilitar las medidas incorporadas.
- Cerrar adecuadamente las sesiones de banca electrónica y compra on line.
- Tener desactivados los servicios de WIFI, Bluetooth y Geolocalización cuando no se estén utilizando.
- Evitar enviar información personal mediante mensajes de texto, chat o correo electrónico.
- Desconfiar y, de ser posible, no abrir ningún link recibido a través de mensajes y/o e-mails que no conozcamos su procedencia.
- Instalar un software de seguridad en el dispositivo móvil.

A esta lista aportada por las empresas de software de seguridad habría que

añadir, el uso únicamente de redes inalámbricas de confianza. Gracias a las funcionalidades que hoy día nos encontramos en cualquier dispositivo Android o IOS podemos crear un punto de conexión a Internet a través de nuestro Smartphone, de tal forma que sea visto por el resto de Smartphones que estén en el radio de alcance como una red inalámbrica. De este modo, si la persona tiene dudosas intenciones, podría ganarse la confianza de los usuarios simplemente poniendo un nombre de cierta credibilidad a la red y, de este modo, todos los datos de las personas que se conecten a la red pasarían por el Smartphone del creador de la red, poniendo en riesgo la seguridad de todos los datos enviados a través de ella.

Red.es (2015) nos ofrece una guía de buenas prácticas:

- Precaución con los enlaces en los que pinchamos. Los creadores de phishing se aprovechan de la poca visibilidad de las pantallas de los Smartphones en las que en ocasiones no se ve una dirección web completa, para engañar al usuario y llevarle a una página falsa, idéntica a la verdadera y conseguir, sus datos de acceso.
- Las preguntas de seguridad que se ponen en las cuentas en ocasiones son fáciles de adivinar lo que supone un gran riesgo, ya que otra persona podría acceder a ellas.
- Evitar la navegación por páginas web sospechosas que ofrecen multitud de servicios gratis, en ocasiones muchos de ellos ilegales.
- Es muy importante configurar adecuadamente la privacidad de todas nuestras cuentas y especialmente de las redes sociales.

2. Iniciativas europeas para la creación de una Internet segura para los menores

En este apartado vamos a examinar y analizar los principales programas que se han realizado, tanto a nivel nacional europeo, relativos al uso de las TIC y Seguridad en la Red. Estos programas y estrategias nos perfilan el momento en que nos encontramos actualmente en la lucha contra los riesgos y peligros derivados de las tecnologías de la información y la comunicación, y más concretamente de Internet.

En España, como país miembro de la Unión Europea, debemos conocer los programas y recomendaciones que surgen desde la Comisión Europea, así como sus motivaciones e iniciativas, en materia de seguridad en Internet para crear una estrategia acorde a ellas.

Sólo conociendo dichas estrategias y sus resultados obtenidos, así como las recomendaciones y conclusiones de expertos nacionales e internacionales, podremos crear una base sólida en nuestra investigación, que nos permita crear una estrategia de intervención adecuada, cuyos resultados sirvan de base científica para futuras investigaciones.

2.1 EU Kids Online I

El 75% de los jóvenes usan Internet bajo la atenta mirada de observadores europeos que quedan asombrados y celebran el uso que hacen los menores de las tecnologías on line. Del mismo modo, otros temen que el uso de estas tecnologías pueda dañarles de algún modo conocido, o no conocido hasta el momento.

Bajo este marco y financiado por el Programa Safer Internet de la Comisión Europea, surge EU Kids Online (2006-2009) con el objetivo de identificar, comparar y obtener conclusiones de las investigaciones europeas, realizadas y en curso, que exploren el uso que hacen los menores de las tecnologías on line.

El objetivo del proyecto EU Kids Online "consiste en mejorar el conocimiento sobre las prácticas y experiencias, de los menores europeos, relativas al riesgo y seguridad en el uso de Internet y las nuevas tecnologías, y de este modo contribuir a la promoción de un entorno digital más seguro para los niños y niñas" (Garmendia, Garitaonandia, Martínez y Casado, 2011, pág. 9).

Las políticas van dirigidas a maximizar las oportunidades que presentan para los menores las tecnologías emergentes y minimizar los riesgos. Para conseguirlo se necesitan hacer estudios e investigaciones que nos aporten pruebas basadas en la evidencia (Livingstone & Leslie, EU Kids Online: Final Report, 2009).

En su primera versión, desarrollada entre el 2006 y el 2009, tenía por objetivo analizar bajo aspectos culturales y contextuales los riesgos del uso de las tecnologías utilizadas en Internet entre los menores de una red de 21 países europeos: Alemania, Austria, Bélgica, Bulgaria, Chipre, Dinamarca, Eslovenia, España, Estonia, Francia, Grecia, Irlanda, Islandia, Italia, Noruega, Países Bajos, Polonia, Portugal, República

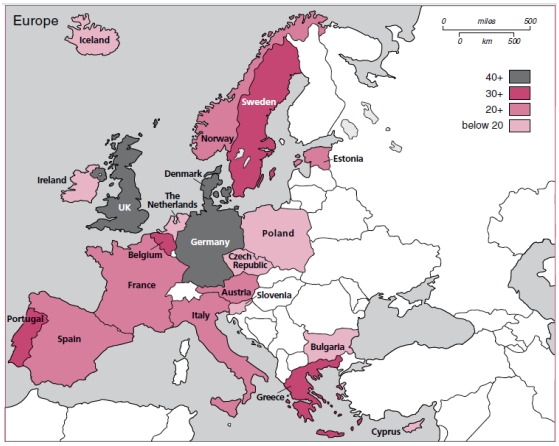


Figura 6 Número de estudios realizados en cada país

Checa, Suecia y el Reino Unido (Livingstone & Leslie, EU Kids Online: Final Report, 2009).

Investigaciones anteriores

Después de haber construido una base de datos de cerca de 400 estudios, se comprobó que las investigaciones realizadas se habían producido de forma desigual en los países analizados, concluyendo que se realizaban mayormente en aquellos países donde existía un mayor número de jóvenes que utilizaban las nuevas Tecnologías de la Información y la Comunicación.

Las investigaciones estaban elaboradas principalmente en Alemania, Reino Unido y Dinamarca y con menor frecuencia en Chipre, Bulgaria, Polonia, Islandia, Eslovenia e Irlanda.

En la Figura 6 podemos apreciar las investigaciones aportadas por cada uno de los países participantes. Los colores utilizados, de más tenues a más intensos, indican los países que han aportado mayor o menor número de investigaciones respectivamente.

No es casualidad, que los países donde más se elaboraban este tipo de estudios o investigaciones es donde existía un mayor interés por conocer los riesgos que derivados del uso de las TIC y más concretamente centrado en Internet.

Objetivos de la EU KIDS ONLINE

Los objetivos prioritarios del proyecto fueron cuatro (Garmendia, Garitaonandia, Martínez y Casado, 2011) :

Identificar y evaluar hallazgos sobre el uso que las/los niñas/os hacen de Internet, así como las principales lagunas en las evidencias base.

Examinar cómo el marco en el que se realizan las investigaciones influye en la agenda de investigación, así como identificar los métodos con mejores prácticas.

Comparar hallazgos a lo largo y ancho de Europa, contextualizando similitudes y diferencias entre los países implicados.

Desarrollar recomendaciones de acciones de políticas públicas que promuevan el uso seguro de Internet basadas en evidencia.

Otros objetivos transversales establecidos en el reporte fueron los siguientes:

Establecer el contexto de la investigación: entender los contextos nacionales e institucionales de la investigación.

Buenas prácticas metodológicas en la realización de investigaciones sobre el binomio –tecnologías y niños- : guiar a los investigadores que afrontan el reto metodológico de los niños que estudian on line, a nivel nacional.

Difusión: divulgar los resultados de la investigación, orientación de los métodos, recomendaciones a las audiencias públicas, académicas y políticas.

EU Kids Online ha centrado el foco de su investigación en la intersección entre: los jóvenes de hasta 18 años y sus familias; las tecnologías on line y en las investigaciones europeas existentes sobre las políticas de uso, riesgos y seguridad de las TIC. El resultado, tal y como podemos ver en la Figura 7, son las oportunidades, riesgos, características de utilización, seguridad, etc..., que los jóvenes experimentan cuando hacen uso de las tecnologías de la información y la comunicación.

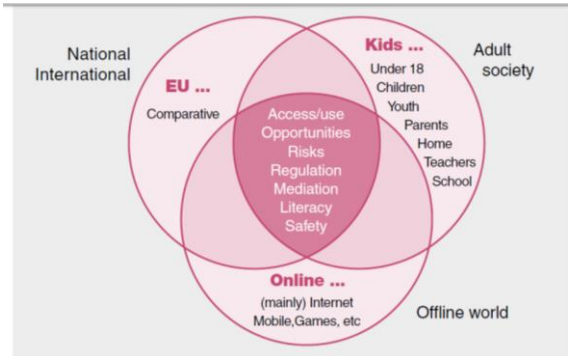


Figura 7 EU Kids Online: Focus del Proyecto

(Livingstone & Leslie, EU Kids Online: Final Report, 2009)

Clasificación de los riesgos on line para los niños

En la Figura 8 podemos ver la clasificación de los riesgos que se realizó en EU Kids Online I. Cada uno de ellos ha sido discutido en los círculos políticos, dando lugar a numerosas iniciativas para hacerles frente.

		Contenido: Receptor de contenidos (Visualiza)	Contacto (Generalmente iniciado por adultos): Participante en actividades on line	Conducta: Perpetrador o víctima de riesgos
RIESGOS	**Comercial**	Spam, mensajes publicitarios, marketing encubierto.	Uso indebido de los datos personales. (Ejemplo: Introduce tu teléfono para…)	Descargas ilegales, violación de los derechos de autor
	Violencia	Acceso a contenidos violentos y agresivos.	Acoso de desconocidos	Acoso o intimidación entre iguales
	Sexual o pornográfico	Acceso a contenidos sexuales y pornográficos	Abusos y chantajes sexuales	Subir material sexual o pornográfico

	Valores	Drogas, racismo, intolerancia, etc.	Persuasión ideológica	Creación de contenidos nocivos (Anorexia, suicidio, etc.)

Figura 8 Riesgos relacionados con el uso de los y las menores en Internet.

(Livingstone & Leslie, EU Kids Online: Final Report, 2009)

Los riesgos han sido clasificados según los "derivados de las actividades de niños y niñas en términos de riesgos de contenido (en los que el niño o niña es receptor), riesgos de contacto en los que el niño o niña participa de algún modo, aunque sea involuntario y riesgos de conducta (donde el niño o niña es actor)" (Garmendia et al., 2011).

Por el momento, no se han logrado conocer la incidencia y la gravedad de cualquiera de los daños a los menores. En investigaciones posteriores se obtendrá más información al respecto, aunque como podremos apreciar quizás aún sea insuficiente.

Análisis resultados obtenidos por EU Kids Online I

En estos años el uso de Internet entre los menores y adultos fue creciendo en todos los países del estudio, siendo en algunos como España un crecimiento vertiginoso, pues el uso por partes de los menores aumentó del 52% al 70% del año 2005 al 2008. Cabe señalar que el porcentaje de personas que hacen uso de Internet se altera a lo largo de estos años entre adolescentes y sus padres, siendo los adolescentes, finalmente, quienes hacen mayor uso de Internet. Por otro lado, se observa que las diferencias de

género van desapareciendo en el uso de Internet mientras que las diferencias debidas a desigualdades económicas persisten en la mayoría de los países.

La exposición a riesgos más repetida en toda Europa, teniendo más incidencia en unos países que otros, por parte de los menores es la exposición de información personal en la red, favorecida por las redes sociales. Siguiendo los siguientes riesgos:

- Exposición de información personal.
- Acceso a contenidos pornográficos.
- Acceso a contenidos violentos o de odio.
- Ser intimidado en línea.
- Recibir comentarios sexuales no deseados.

El riesgo menos común es el encuentro con personas conocidas en Internet, aunque se considera el riesgo más peligroso.

Estatus socioeconómico y género

En cuanto a la variable socioeconómica, se hace notar que a pesar que las familias con mayores recursos económicos tienen más posibilidades de proporcionar acceso a Internet a sus hijos e hijas, son los menores provenientes de familias con menos recursos económicos los que están más expuestos a los riesgos de la red. También se dan diferencias de género, siendo los chicos quienes se encuentran o crean, con mayor frecuencia, conductas de riesgo, mientras que las chicas son más afectadas por los contenidos y contactos de desconocidos.

Clasificación por países

Los países fueron clasificados en, países de "alto riesgo"; "riesgo medio" y "bajo riesgo". Para ello, se ha tenido en cuenta el uso de Internet y la exposición a riesgos al conectarse a la red. Los países dentro de "alto riesgo" están situados por encima del promedio europeo. Los países de "riesgo medio" están en torno al promedio del resto de países. Y los países de "bajo riesgo" están por debajo de la media europea. Además, se observó una correlación positiva entre el uso y el riesgo. Así se obtiene que:

- ✓ Los países del norte de Europa tienen un alto uso – alto riesgo.
- ✓ Los del sur de Europa, tienen bajo uso – bajo riesgo.
- ✓ Los países del este de Europa tienden a menor uso – menor riesgo.

	Children's internet use		
Online risk	**Low (< 65%)**	**Medium (65%-85%)**	**High (> 85%)**
Low	Cyprus Italy	France Germany	
Medium	Greece	Austria Belgium Ireland Portugal Spain	Denmark Sweden
High		Bulgaria Czech Republic	Estonia Iceland Netherlands Norway Poland Slovenia UK

Figura 9 Clasificación de países por uso de Internet y exposición a los riesgos.

(Livingstone & Leslie, EU Kids Online: Final Report, 2009)

Recomendaciones políticas

EU Kids Online, ofrece algunas recomendaciones según los resultados de sus investigaciones.

Las políticas de e-integración deben centrarse en los países donde el uso de Internet es más bajo (Italia, Gracia y Chipre), especialmente en los segmentos de la población con menos recursos económicos. Además, el 25% de menores europeos que no hacen uso de Internet y se debe de facilitar y conseguir su inclusión digital.

Se considera muy importante tener en cuenta la tendencia existente de mayor uso – mayor riesgo, para aumentar paulatinamente el empoderamiento y la seguridad con la que la población hace uso de Internet. Por el contrario, las estrategias que pretenden evitar que los menores se expongan a los riesgos de Internet mediante la prohibición, la restricción de sus derechos y oportunidades, podrían tener consecuencias negativas para los jóvenes que deberían ser valoradas.

El equilibrio de estos objetivos en conflicto requiere la combinación de la regularización, alfabetización digital y la mejora del diseño de la interfaz. El acompañamiento en el aprendizaje y uso de las TIC también puede resultar positivo y reducir los riesgos, mediante el uso responsable y las actividades valiosas que presentan oportunidades. También se reconoce la importancia de la provisión de infraestructuras TIC en las escuelas, formación del profesorado y la adaptación del currículo de los centros.

Familias

En el momento del estudio se contaba con pocos datos respecto a los padres, motivo por lo que el estudio se apoyó en el análisis de la encuesta Eurobarómetro del 2008. En ella se aprecia que la preocupación de los padres con respecto a la seguridad on line de sus hijos es alta, lo que parece estimular a la puesta en práctica de diferentes

formas de protección ya se traduzca en menor exposición al riesgo o mejor recuperación al impacto de un riesgo. Sin embargo, no se conoce la eficacia de éstas iniciativas.

Al preguntar a los padres que riesgos les preocupan a sus hijos, en el estudio realizado por el Eurobarómetro (2008) nos encontramos que:

- El 65% les preocupa que sus hijos vean imágenes explicitas sexuales o violentas.
- El 60% que puedan ser víctimas de acoso sexual on line por adultos.
- El 55% que accedan a información que pueda dañarles como páginas con contenidos sobre anorexia, bulimia o suicidio.
- Al 54% les preocupa que sus hijos sufran ciberbullying.
- Al 53% que sus hijos sean ignorados por otros niños y adolescentes.
- Al 47% que den información privada a través de la web.

Curiosamente el 25% de los padres les preocupa mayormente la exposición a riesgos de los más pequeños de los menores y de las chicas, mientras que los resultados obtenidos muestran que los chicos y adolescentes se exponen mayormente a los riesgos.

Aunque de momento tan solo sean hipótesis, la exposición que experimentan mayormente los chicos y los adolescentes puede deberse a que los adolescentes hacen mayor uso de Internet y, por otro lado, que los chicos se sienten más invulnerables o son menos precavidos que las chicas.

Se ha detectado un importante porcentaje de familias que no disponen de los conocimientos necesarios para hacer frente a los riesgos de la red, lo que les coloca en una situación de vulnerabilidad no sólo a ellos como adultos, sino también a sus hijos que no recibirán el apoyo que necesitan en casa para utilizar las de manera segura.

La Figura 10 muestra la relación que presenta cada país entre restricción y mediación de los padres en el uso de Internet de sus hijos e hijas.

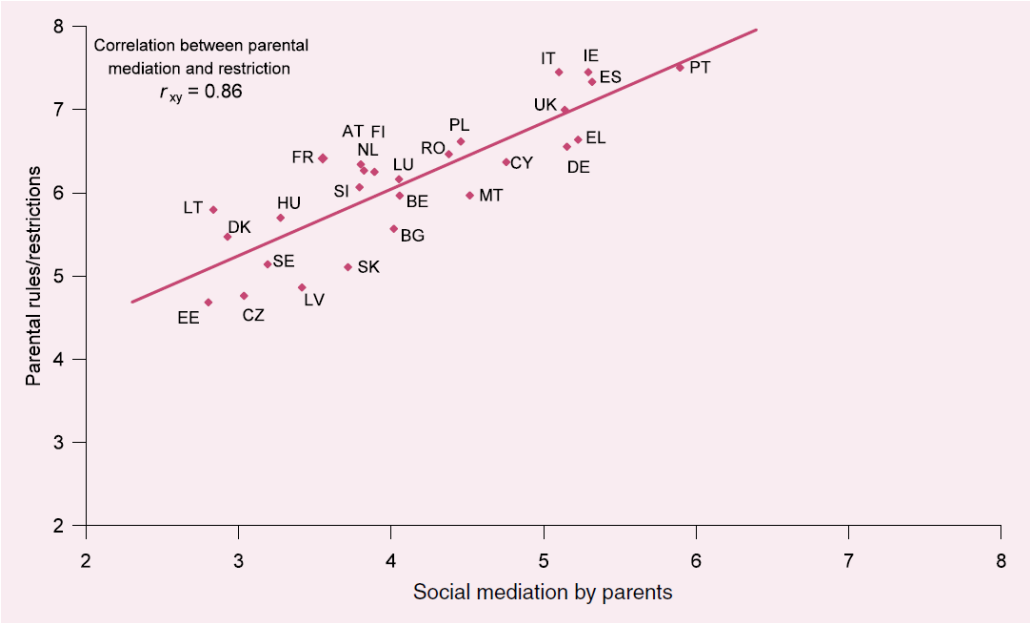


Figura 10 1Correlación por países entre restricción y mediación de los padres en el uso de Internet de sus hijos e hijas

(Livingstone & Leslie, EU Kids Online: Final Report, 2009)

Más adelante veremos el papel que adquieren los padres y madres en el uso que hacen sus hijos e hijas de las TIC, y más concretamente de Internet, ya que es fundamental en el aprendizaje y en el uso responsable y seguro.

Si queremos que los menores estén seguros al conectarse a Internet no basta con seguir indicaciones básicas sobre el uso de la red, sino que es necesario regular el entorno desde el que se conectan los jóvenes mediante la aplicación de leyes que protejan sus derechos; desarrollar software y diseño web adaptado a sus necesidades; que los buscadores muestren resultados de búsqueda adecuados para menores; creación de recursos de seguridad on line; etc. Les podemos enseñar el modo de utilizar los

recursos de manera adecuada para garantizar su seguridad, pero los recursos que obtengan on line también tienen que estar adaptados a sus necesidades y características.

Sensibilización de la sociedad europea

Según EU Kids Online, las prioridades de sensibilización de la población deben centrarse en los países catalogados de alto riesgo (Estonia, Países Bajos, Noruega, Polonia, Eslovenia y Reino Unido). También se debe prestar especial atención a los países donde se tiene acceso a Internet recientemente, donde las posibilidades de acceso crecen más rápidamente que las habilidades para utilizar los recursos en Internet (Bulgaria, Estonia, Grecia, Polonia y Portugal). La última variable considerada prioritaria es la de los jóvenes que usan más frecuentemente Internet que sus padres (Hungría, Malta, Polonia y Rumanía).

Dentro de los usuarios de Internet, debe prevalecer la atención a los colectivos más vulnerables, siendo los niños más pequeños sobre quienes deben priorizarse las estrategias de intervención. Además, se debe tener en cuenta las diferencias de género y trabajar de manera adaptada con cada sexo. Por otro lado, las familias con menos recursos y las escuelas y barrios más desfavorecidos también se consideran prioritarios.

Víctima o perpetrador

En cuanto a la escena política, debe ir más allá de la división entre víctimas y adultos perpetradores de riesgos. El horizonte de Internet es más amplio. Los niños pueden ser víctimas, pero también pueden ser perpetradores y, en ocasiones, los perpetradores se convierten en víctimas y viceversa. Por otro lado, los padres en ocasiones no tienen los conocimientos necesarios para proteger a sus hijos en red, para

aportarles la información que necesitan para no exponerse a los riesgos o para establecer restricciones que velen por la seguridad de sus hijos. Además, no está claro que las estrategias utilizadas por los padres sean eficaces para reducir su exposición al riesgo o para mejorar su capacidad de hacerles frente. Los padres utilizan las estrategias que consideran mejores para proteger a sus hijos sin conocer sus resultados lo que demuestra una carencia que debe ser atendida.

Recomendaciones de la investigación

De la investigación, además, se desprenden las siguientes recomendaciones que deben tenerse en cuenta:

Los riesgos pueden evolucionar o surgir otros nuevos, como autolesiones, suicidio, pro-anorexia, drogas, adicción, etc.

Es necesario actualizar las investigaciones sobre los menores.

Conocer la evolución de los contenidos emergentes, servicios, dispositivos y plataformas. Pueden suponer un cambio en la exposición y afección de los riesgos.

Entender el desarrollo de las habilidades de búsqueda, navegación e interpretación crítica de los menores.

Estrategias de padres e hijos para responder ante los riesgos. Pautas o guías de respuesta.

Identificar a los jóvenes más expuestos a los riesgos.

Evaluar la eficacia de las técnicas para paliar los efectos nocivos de las TIC, la mediación parental, la alfabetización digital y otras medidas de sensibilización y seguridad, en términos de la reducción de riesgos. Esto puede ser diferente para niños de diferentes contextos culturales.

En la Figura 10 podemos ver estadísticas obtenidas de las encuestas del Eurobarómetro que fueron encargadas por el Programa Safer Internet para proporcionar un marco cuantitativo para los hallazgos de EU Kids Online. La Figura 10 nos muestra, clasificado por países, el porcentaje de población que dispone de acceso a Internet por banda ancha, los menores que utilizan Internet divididos por grupos de edades y el porcentaje de padres que utilizan Internet. También muestra los resultados obtenidos en 2005 de jóvenes y padres que utilizaban en Internet.

Para que las deliberaciones políticas estén basadas en la evidencia y directamente comparadas con las investigaciones de cada país participante es vital identificar similitudes entre los países europeos y regionales, o factores específicos de cada país.

Después de tres años de investigación, identificando, revisando y extrayendo información de investigaciones e implicaciones políticas claves para crear la base de los conocimientos existentes en Europa, se concluye que todavía queda mucho por entender, especialmente si tenemos en cuenta el ritmo de cambio tecnológico y social.

Programa Safer Internet Plus (2005-2008) fue el encargado de los "proyectos de mejora de los conocimientos que tienen como objetivo aumentar el conocimiento relevante sobre las tecnologías on line más seguras", específicamente para fortalecer la base del conocimiento mediante la realización de "un estudio cuantitativo comparable sobre el uso que hacen los menores de las tecnologías on line, analizando la percepción de los padres y madres del uso que hacen sus hijos de las tecnologías". Posteriormente, se asigna la coordinación de UE Kids On line a la 'London School of Economics and

Political Sciences' que, tras la experiencia de EU Kids Online I (2006-2009), desarrolló posteriormente EU Kids Online II durante los años del 2009 al 2011.

2.2 EU Kids Online II

En la anterior investigación de EU Kids Online, se identificaron una amplia gama de riesgos, expuestos en la Figura 1. Es llamativo que los riesgos que más preocupan a los menores, con frecuencia, no coinciden con los que más alarma generan y más ansiedad provoca a los adultos. También destaca que, cuanto más se conectan a Internet, es más probable que encuentren riesgos, bien accidental o deliberadamente. Se podría interpretar que a más uso, mayor nivel de conocimiento de navegación por Internet y menor exposición a los riesgos, sin embargo, conocer en profundidad una herramienta digital o ser experto en la navegación on line no implica que se utilice de manera más segura.

EU Kids Online II (2009-2011) es un proyecto de investigación diseñado para examinar las experiencias de uso, riesgos y seguridad on line de niños, niñas, padres y madres en Europa. El proyecto tiene los siguientes objetivos (Garmendia, Garitaonandia, Martínez y Casado, 2011)

- Alcanzar conclusiones actuales que permitan conocer la incidencia de los riesgos on line entre los menores europeos.
- Señalar con precisión los colectivos más vulnerables entre los menores y cuáles son los factores de vulnerabilidad.
- Examinar la eficacia y las estrategias de regulación parental y las respuestas de los menores a los riesgos.

En el presente análisis de la encuesta realizada en 2011 se identificarán factores de riesgo en el uso de las TIC, más concretamente de Internet para los menores, lo que no quiere decir que vaya a pasar a formar parte en las próximas agendas políticas para su erradicación. Quizás, porque los costes sean demasiado elevados para el menor (p.e. puede suponer que sus libertades sean restringidas debido a la prohibición de acceso a contenidos o la supervisión obligada de adultos) o para el estado (suponiendo un gasto de implementación considerado excesivo para los beneficios que propone) o para la industria (exceso de regulación). Se puede observar que el debate está abierto y la valoración de la importancia dependerá de quien responda (Garmendia et al., 2011, pág. 10).

En nuestro caso, nos limitaremos a analizar los resultados obtenidos en la investigación, pero es necesario tener en cuenta que en la vida cotidiana de los niños, los padres y las madres toman decisiones que pueden afectar a sus hijos permitiéndoles exponerse a riesgos.

A diario, los niños juegan, se sociabilizan, toman decisiones de manera autónoma, hacen deportes, cruzan carreteras, montan en bici o utilizan objetos punzantes sin que ello suponga un problema. En este momento, un padre o una madre, puede estar enseñando a su hijo a cruzar por el paso de cebra, a utilizar un cuchillo correctamente o quizás le enseñe a utilizar el monopatín o la bicicleta. Es posible que alguno de ellos tema que su hijo se dañe, sin embargo, procura dotarle de las herramientas necesarias para que no se dañe y, si se cae de la bici o se corta con el cuchillo, le ayuda a recuperarse, pero unos días después volverá a intentarlo. La familia valora la magnitud de la peligrosidad y decide permitir al joven realizar la actividad.

Considera que el aprendizaje es positivo para el pequeño y, por tanto, que la exposición al riesgo es necesaria. Bajo este enfoque se desarrolla la perspectiva adoptada por el informe que analizamos a continuación.

Se debe tener en cuenta que se trata de explorar las experiencias on line de los menores y comprender cómo las actividades on line de los menores encajan en un entorno más amplio –tanto on line como off line-, de tal manera que permita ver qué factores contribuyen a aumentar o disminuir el riesgo (Garmendia et al., 2011, pág. 10).

Se debe puntualizar que la investigación se realizó con un total de 25420 niños y niñas usuarios de Internet, de un total de 25 países participantes, así como a uno de sus padres. Como puede observarse en la Figura 11, la muestra tomada de los países europeos no corresponde con la Unión Europea.

Figura 11 Países participantes en el Euro Kids On Line II

(Grupo de Investigación EU Kids Online)

Alcance del proyecto de EU Kids Online

"La parte sombreada de la Figura 12 muestra el alcance del proyecto EU KIDS ONLINE que abarca una parte de este dibujo. Específicamente, estudia el uso y las actividades (experimentadas por los niños y niñas de Europa), a través de su relación con determinados factores que hipotéticamente aumentan la probabilidad de sufrir riesgos (que afectan a una menor proporción de los niños). Finalmente, el proyecto analiza los resultados para los niños/as en términos de percepción del daño o, desde una perspectiva más positiva, cómo afrontan los niños/as estos factores de riesgo (que hipotéticamente afectan a una proporción aún menor)" (Garmendia, Garitaonandia, Martínez y Casado, 2011)

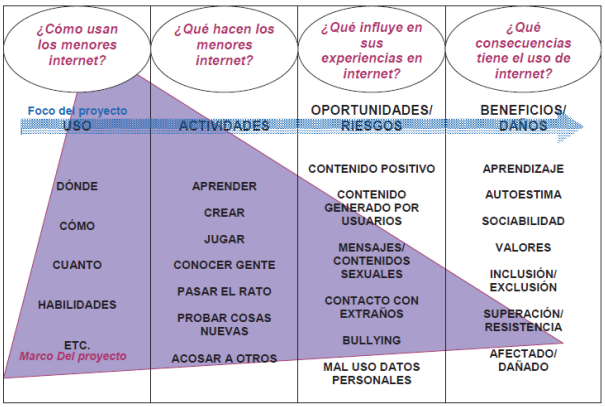


Figura 12 Posibles consecuencias de las actividades on line

(Garmendia et al., 2011)

Factores ambientales, Exposición a riesgos y Afección del daño

Existen factores ambientales que rodean al joven que influyen en las actividades que realiza y, por lo tanto, intervienen en que las experiencias vividas sean positivas/beneficiosas o negativas/perjudiciales. Por ejemplo, que haya personas

conectadas con las que quiero contactar hace que el joven se conecte a determinados servicios o, dependiendo del lugar desde el que se conecta -en privado desde su habitación o en el salón delante de su familia- puede propiciar que el joven realice unas u otras actividades. Por lo tanto, se puede decir que los factores que rodean al joven en el momento en que se va a conectar a la red son determinantes en las actividades que realizará en Internet.

Algunos de estos factores pueden influir en que aumente la probabilidad de exposición a riesgos, como el acceso a contenidos inapropiados u otros sitios web en los que asistan personas que hagan apología de conductas inmorales o violentas.

Hasta el momento, no se conoce el daño que puede causar a un joven la exposición a alguno de los riesgos de la red. Dependiendo del riesgo al que el o la joven se exponga, el daño que puede causarle difiere. Además, la afección que tiene un riesgo para un joven depende del joven en sí mismo y de las circunstancias que le rodean. No afecta del mismo modo a unas personas que a otras ser insultado a través de la red, visualizar pornografía, etc.

Aunque no es posible establecer conexiones directas entre las entre experiencias de riesgo y experiencias de daño, sí que es posible obtener algunas especulaciones o hipótesis. Garmendia et al. (2011) afirman que “es más probable que los jóvenes solitarios sean más acosado por sus iguales y, así mismo, se sientan más afectados por este acoso". Por otro lado, los niños tienden a exponerse más a la pornografía, lo que les hace más vulnerables al riesgo que las niñas. Sin embargo, las niñas se sienten más disgustadas por esa exposición, pudiendo sufrir un mayor daño. Según esto, podemos

deducir que dependerá del riesgo, de los factores que rodean a la persona, del sexo y de la edad, que exista mayor o menor probabilidad de daño.

Del mismo modo, las condiciones ambientales pueden propiciar que los jóvenes accedan a sitios web que representen una "oportunidad" porque fomenten la lectura, beneficien la creatividad o propicien comunicación positiva entre jóvenes. En este caso, las condiciones ambientales pueden propiciar que el joven experimente experiencias positivas y enriquecedoras.

Algunas experiencias vividas en la red no pueden simplificarse como 'buenas o malas' basándose en sus características intrínsecas, sino que dependerán de cómo se vivan y experimenten lo que les convierta en una experiencia positiva o en un factor de riesgo. Este podría ser el caso de las redes sociales, que se analizará más adelante.

En la Figura 13 se puede apreciar la diversidad de factores que pueden influir sobre las experiencias de los niños y las niñas al hacer uso de Internet. En el informe "Riesgos y seguridad en Internet: Los menores españoles en el contexto europeo" se diferencian tres niveles que inciden sobre los menores, de los que hemos ido comentando brevemente:

- Factores demográficos (edad y género), estatus socioeconómico y factores psicológicos de la persona (tendencia a correr riesgos, estabilidad emocional, etc.).
- Factores sociales que median las experiencias on line y off line de los menores, especialmente padres-madres, profesorado y amistades.

- El contexto nacional: factores económicos, sociales y culturales. El análisis de estos factores pretende tratarse en un informe posterior.

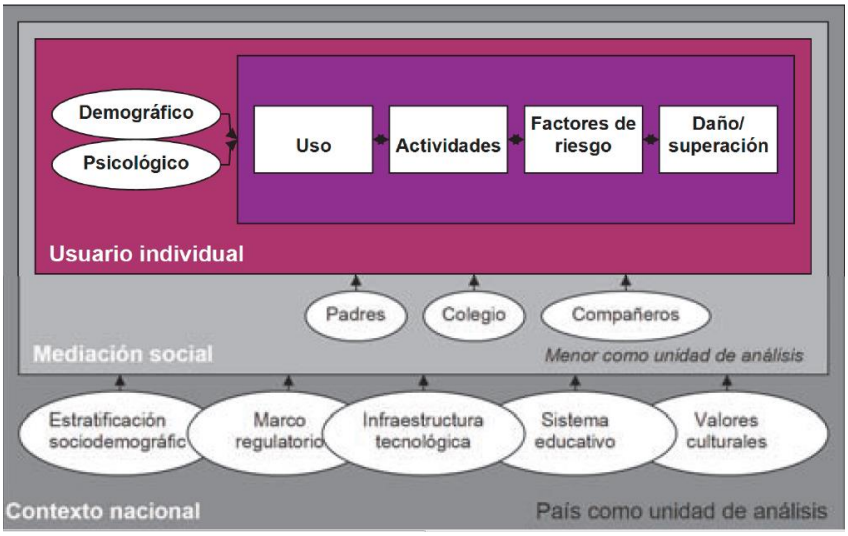


Figura 13 Relaciones de uso, actividades, y factores de riesgo que pueden dañar al menor (Garmendia et al., 2011).

"Los resultados de esta investigación sirven de base de evidencias a las iniciativas políticas sobre las que se sustenta el programa Safer Internet de la comisión europea y de otras organizaciones nacionales e internacionales." (Garmendia et al., 2011).

Conclusiones de EU Kids Online II

En los resultados del proyecto se emplea un diseño comparativo en base a las siguientes variables:

- Las experiencias on line de los menores, diferenciando cuando se conectan desde diferentes localizaciones y con diferentes dispositivos con conexión a Internet.

- Diferencia entre las variables de género, edad y estatus socioeconómico, analizando las diferencias y las semejanzas encontradas en cada una de ellas.
- Los riesgos experimentados por los menores cuando están conectados a Internet.
- Se observa la percepción de los daños sufridos que tienen los menores.
- Los roles de los menores al ser víctimas de uno de los riesgos incluidos y cuándo son causantes de esos riesgos contra otros cibernautas.
- Percepción de los riesgos que tienen los menores y sus padres.
- Además, se compararán los datos obtenidos en los países que formas parte del estudio.

Resultados

El 84% de los menores españoles acceden a Internet desde sus casas, lo que sitúa a las familias en lugar privilegiado para asesorarles, guiarles y compartir experiencias positivas, alejadas de los riesgos de Internet. Sin embargo, como hablaremos más adelante, los limitados conocimientos digitales de padres y madres no eliminan muchas situaciones de vulnerabilidad.

Por otro lado, el 42% se conectan a Internet en un entorno privado, lo que dificulta a los padres la supervisión y acompañamiento de sus actividades digitales. Aun siendo un porcentaje significativo, dicho valor se sitúa por debajo de la media europea que aumenta hasta el 49%. Es por ello necesario prever medidas de sensibilización y asesoramiento a las familias sobre la importancia del acompañamiento y apoyo en el medio digital a los menores para evitar que sigan aumentando estas cifras y alcancen la media europea o la superen como es el caso de Dinamarca que llegan al 74% de los jóvenes que se conectan en entornos privados de sus casas. Según los resultados

obtenidos, en la mayoría de países analizados, prácticamente la totalidad de los jóvenes se conectan desde sus casas. En el caso de España los menores que se conectan desde casa ascienden al84%, lo que supone que el 50% de los menores que se conectan desde sus hogares acceden en privado a Internet, superando así la media europea.

Dispositivo de acceso a Internet	% menores que lo usan
PC compartido	59
PC propio	30
Televisión	2
Teléfono móvil	6
Consola de videojuegos	8
Ordenador portátil compartido	30
Ordenador portátil propio	27
Otro dispositivo móvil	3
Número medio de dispositivos de acceso a Internet	2

Figura 14 Uso de los dispositivos con acceso a Internet

Es llamativa la notable diferencia en dispositivos de acceso que utilizan los menores en España, frente a los europeos. En el caso de la conexión a Internet a través de videojuegos en Europa se conectan el 26% de jóvenes frente al 8% los españoles. Es aún más llamativa la conexión a Internet a través del teléfono móvil que se sitúa en un 6% en España frente al 31% de los europeos. Lo mismo ocurre en el caso de la conexión

mediante el uso de televisión o de otro dispositivo móvil situándose en el 32% y 12% respectivamente en Europa.

En el caso de la conexión a Internet a través del teléfono móvil se ve como los teléfonos móviles con conexión a Internet se han expandido por los países europeos con antelación de hacerlo en España, así como la facilidad de acceder a Internet a través del móvil. En este caso, podemos pensar que es necesario que se den simultáneamente varios factores para aumentar el número de menores que se conectan a Internet a través de los dispositivos móviles. Por un lado, se necesita la adquisición de dispositivos móviles con conexión a Internet y, por el otro, servicios de conexión a Internet a precios razonables. Aun así, la importancia de estos factores en el acceso a Internet a través de dispositivos móviles es tan solo una hipótesis.

Es importante señalar que en este informe no se analizan las variaciones en la exposición a riesgos de los menores en la localización o utilización de unos u otros dispositivos para conectarse a Internet.

Edad, género y estado socioeconómico

Una de las conclusiones de este trabajo es que la edad es una de las variables que más influyen en el tiempo y tipo de uso, y en la exposición a riesgos que los menores experimentan en Internet.

Se puede observar en la Figura 15 que a mayor edad del joven, mejor preparado está para hacer frente a los riesgos escrutados. También se observa diferencias significativas según el sexo de los menores. Por ejemplo, las niñas afirman saber en mayor porcentaje que los niños bloquear a alguien en Internet o cambiar el perfil de

privacidad de su red social, al contrario que ocurre con el bloqueo de spam o el borrado del historial del navegador.

A través de los datos obtenidos, es posible formular algunas hipótesis, como por ejemplo: en función del género, chicos o chicas tienen mayor conocimiento de aquellas herramientas que otorgan más importancia o que conocen las herramientas que les son más útiles porque se exponen en mayor medida a ese riesgo. Esta última, nos referimos al bloqueo de personas no deseadas, de spam o borrado del historial.

Un dato especialmente significativo es que el 90% de los menores entre 15 y 16 años afirman tener un perfil en las redes sociales, pero también los menores entre 11 y 12 años afirman tenerlo, a pesar de no tener edad legal de acceso a la mayoría de redes sociales, edad que en España se sitúa en 14 años salvo en las redes sociales que son específicas para niños. Tal y como afirman Melchor Gómez et al. (2015a), "las redes sociales son un fenómeno social, lo son especialmente y de manera más acusada entre los jóvenes, que son el sector con mayor tasa de utilización".

	11-12 años		13-16 años		
% que afirma saber...	Niños	Niñas	Niños	Niñas	Todos
Bloquear mensajes de alguien con quien no quieres contactar	42	50	77	87	70
Encontrar información de cómo usar Internet de forma segura	42	40	77	71	63
Poner en favoritos una web	65	61	81	82	76
Cambiar los perfiles de privacidad de la red social	30	25	66	72	55
Comparar diferentes webs para contrastar información	46	47	68	67	61
Borrar el registro de las páginas visitadas	25	21	61	57	47
Bloquear anuncios o spam indeseados	38	32	62	57	52
Cambiar las preferencias de los filtros de contenido	11	13	33	34	27
Número medio de habilidades	3,0	2,9	5,2	5,2	4,5

Figura 15 Datos sobre las habilidades en la red que poseen los menores

(Garmendia et al., 2011)

Exposición a riesgos

En cuanto a la exposición a distintos riesgos, se observa que los menores de edad más avanzada están más expuestos a visualizar imágenes con contenidos sexuales, sufrir ciberbullying o acceder a contenidos inapropiados. En el último caso, la diferencia es menos significativa. Sin embargo, son los menores más jóvenes los que afirman sentirse más afectados o disgustados por la afección de estos riesgos.

Según los datos obtenidos, se puede concluir que los menores de más edad están más expuestos, mientras que los menores de menor edad están menos capacitados para afrontarlos. Hay que tener en cuenta que la variable de frecuencia de uso y acceso a Internet podría también tener valor en la mayor exposición a riesgos como hemos hablado con anterioridad.

En cuanto a las diferencias de género, se obtiene que los niños están más expuestos a la pornografía en Internet y a la recepción de mensajes sexuales. Sería interesante conocer si en este último dato influye la intención o acción del joven, es decir, si las acciones del joven en la web propicia que el joven pueda recibir mensajes sexuales. Por otro lado, las niñas sufren más a menudo ciberbullying y acceden a páginas proanorexia y probulimia, mientras que los niños acceden a páginas que incitan al odio y la violencia.

En cuanto a la influencia de los riesgos sobre los menores, las niñas afirman sentirse más disgustadas, sin embargo, se debe tener en cuenta que las respuestas de los niños a estas preguntas pueden estar condicionadas por algunos factores de convención social que lleven a los niños a no admitir sentirse disgustados o molestos por estos contenidos (Garmendia et al., 2011).

En la Figura 16, que muestra los jóvenes españoles que han experimentado alguno de los riesgos consultados, podemos observar que el 35% de los menores han sufrido alguno de estos riesgos. El riesgo que más afecta es el contacto con personas desconocidas fuera de la red, que afecta al 21% de los menores, siguiéndole de cerca el acceso a contenidos peligrosos (páginas probulimia y proanorexia, que incitan al odio o a la violencia, etc.). En primer caso, además, tenemos que el 9% de los menores que conocen a alguien a través de Internet terminan conociéndole en persona. Este dato, que puede resultar alarmante, por el riesgo que podría generar que los menores puedan ser engañados por pederastas o con otras personas peligrosas para ellos y conocerse personalmente, está agrandado por los contactos que generan los menores entre iguales

sin ningún riesgo y que además les permitan fomentar la socialización y hacer uso de sus herramientas sociales y de comunicación.

%	Edad				Todos
	9-10	11-12	13-14	15-16	
Ha visto imágenes sexuales en los últimos 12 meses en internet	8	3	15	17	11
Ha recibido mensajes violentos o desagradables en los últimos 12 meses por internet	1	3	6	7	4
Ha visto o recibido mensajes sexuales en los últimos 12 meses por internet	n.r.	3	10	13	9
Ha contactado en internet con alguien que no conoce en persona	9	13	23	33	21
Se ha citado con alguien en persona a quien ha conocido a través de internet	5	4	8	17	9
Ha accedido a contenidos generado por otros usuarios potencialmente perjudiciales en los últimos 12 meses	n.r.	7	20	29	19
Ha sufrido el uso indebido de sus datos personales en los últimos 12 meses	n.r.	7	13	8	10
Ha sufrido uno o más de los riesgos anteriores	**12**	**25**	**45**	**54**	**35**
Ha actuado de una manera violenta contra otros en internet en los últimos 12 meses	1	1	2	6	3
Ha enviado mensajes sexuales de algún tipo a través de internet en los últimos 12 meses	n.r.	1	2	2	1
Ha hecho algo de esto	**1**	**2**	**4**	**7**	**4**

Figura 16 Riesgos percibidos por los menores en la red según grupos de edad

(Garmendia et al., 2011)

Riesgo y daño

Hemos visto que la exposición a riesgos no implica necesariamente que existan daños en los menores, por lo que en desarrollo del proyecto se ha analizado el vínculo entre ambos. Es necesario tener en cuenta que los resultados encontrados están basados

en la percepción del daño de los menores y están obtenidos de la media de los países participantes en el proyecto:

El 12% de los jóvenes entre 9 y 16 afirman haber sido dañados o molestados por alguno de los riesgos contemplados.

1 de cada 12 niños han conocido en persona a un contacto conocido a través de la web, sin embargo, rara vez esta experiencia desencadena algún daño.

Los chicos y los adolescentes están más expuestos a las imágenes con contenido sexual y las chicas están más expuestas a recibir mensajes on line que les dañen de algún modo.

El 41% se han expuesto en alguna ocasión a alguno de los riesgos.

Los riesgos incrementan con la edad del menor. El 14% de niños entre 9 y 10 años se han enfrentado a alguno de los riesgos, el 33% entre adolescentes de 11 y 12 años y el 63% de jóvenes entre los 15 y 16 años.

La Figura 17 nos permite visualizar la percepción del daño recibido que experimentan los menores que han afirmado haber experimentado alguno de los riesgos consultados.

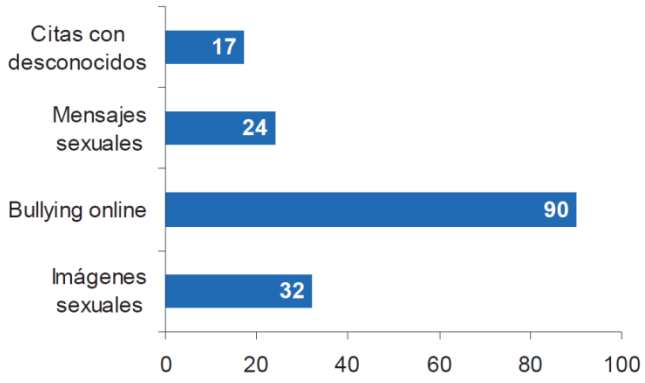


Figura 17 Percepción del daño por parte de los menores

(Garmendia et al., 2011)

Se observa una gran diferencia entre la percepción de la afección de daño de los jóvenes, según el riesgo experimentado. Mientras que en el caso del Ciberbullying nueve de cada diez jóvenes afirman haberse 'sentido molestos o disgustados' por el suceso experimentado, en el caso de las citas con desconocidos desciende al 17%.

Partiendo que la información obtenida es la percepción de la afección del daño del menor, podemos intuir que aunque los riesgos analizados pueden ser considerados perjudiciales en sí mismos, en la mayoría de los casos no desembocan en ningún perjuicio para el menor.

También debemos tener en cuenta que la percepción del daño de unos riesgos a otros puede ser, en intensidad, muy diferentes. Es decir, el daño experimentado por los menores que afirman sentirse disgustados al ver imágenes sexuales no tiene, necesariamente, que tener la misma intensidad que cuando se sufre acoso a través de la red. Por lo tanto, no podríamos extrapolar la afección de los daños entre sí, al igual que no podemos conocer las consecuencias concretas de la exposición a los riesgos o de la afección de los daños.

Estatus socioeconómico

Livingston y Haddon (2007) vieron necesario analizar el estatus socioeconómico de los participantes con la intención de poder reflejar las posibles diferencias derivadas de situaciones sociales y/o económicas más o menos favorecedoras de los sujetos, del mismo modo que ha ocurrido en investigaciones anteriores sobre la brecha digital. La conclusión fue que, en general, no se detectaron diferencias significativas entre los menores de diferentes estatus socioeconómico,

excepto por una mayor exposición a imágenes con contenido sexual y mayor incidencia del ciberbullying entre los menores de estatus socioeconómicos más elevados. Si llama la atención, la percepción de conocimientos respecto a sus padres y madres que tienen los menores. Mientras que en los hogares de niveles socioeconómicos elevados sólo el 22% afirman saber más de Internet que sus padres, en los hogares de niveles socioeconómicos más bajos el 64% hacen esta afirmación. Estos datos pueden implicar que los menores cuanto menor es el nivel socioeconómico de la familia en menor medida ven a sus padres y madres como personas de referencia en este terreno, lo que dificulta la intervención de los padres como mediadores cuando sus hijos hacen uso de Internet.

Víctimas o perpetradores

La perspectiva del perpetrador y la de la víctima puede ser muy distinta. Mientras una persona se está divirtiendo, otra persona puede sentirse herida y en esta acción puede, o no, haber intención de llegar a los efectos resultantes de la interacción entre dos personas. Esta situación, aunque puede parecer muy simplista, se da a menudo a través de redes sociales entre menores. La distancia que marcan las TIC hace que el menor perpetrador no sea consciente de los efectos de sus actos sobre otros jóvenes.

En ocasiones, los jóvenes pueden navegar por Internet o sociabilizarse a través de las redes sociales que manejan y pueden acabar dañando a otro joven. Puede que esta conducta pretenda herir a la otra persona o simplemente responda a la necesidad de hacer algún comentario jocoso para ganarse el favor de las otras personas que pueden acceder a la información expuesta en la red, o bien demostrar a la otra persona sus habilidades cómicas.

Basándonos en los resultados del estudio es especialmente llamativo que el 15% de los menores afirman haber sufrido bullying o ciberbullying pero tan sólo el 9% confiesan haber acosado a otro menor. Si únicamente tenemos en cuenta el ciberbullying el 5% afirma haber recibido mensaje de acoso y sólo el 3% confirman haberlos enviados.

Se ha detectado que una variable significativa en el envío y recepción de mensaje de acoso es la edad, dando como resultado que la frecuencia aumenta al aumentar la edad del menor. Además, es llamativo que en la investigación se demuestra la conexión entre ambas categorías, víctima y perpetrador (Hinduja & Patchin, 2009).

Perspectivas sobre el riesgo: padres e hijos

De toda la información obtenida en este informe focalizaré mi atención en la percepción de los riesgos de Internet que tienen los padres y madres de sus hijos. En anteriores investigaciones se obtuvo que existían grandes diferencias sobre la percepción del riesgo existente en la red entre padres e hijos. En este caso, vemos que las percepciones de ambos en el momento del estudio se acercaban bastante. Mientras que tiempo atrás se obtuvo que los padres solo valoraban de manera moderada los riesgos que sus hijos experimentaban en Internet, en esta investigación se dedujo que los padres son cada vez más conscientes de las experiencias que sus hijos tienen en Internet.

Esta conclusión hace pensar que las campañas de sensibilización están teniendo éxito, sin embargo, estos resultados se obtienen, en parte, gracias a padres y madres que afirman no haberse enfrentado a los riesgos.

Cuando la pregunta se centra en los riesgos experimentados por sus hijos parece que los padres siguen sin conocer las experiencias de sus hijos en la red, mostrando cierto grado de incertidumbre al respecto. Y este desconocimiento aumenta de manera inversamente proporcional a la edad de los niños. Por ejemplo, los padres no son conscientes de la exposición de los hijos menores más pequeños a imágenes sexuales en relación con los hijos adolescentes.

Dado que Internet es utilizado por los niños en casa, debe ser una prioridad política aumentar los niveles de concienciación de los padres sobre los riesgos que pueden encontrar los jóvenes en la red.

Además, teniendo en cuenta los resultados EU Kids Online I y EU Kids Online II, éstas políticas deben prestar especial atención a las familias más desfavorecidas social, cultural o económicamente, además de a aquellas con menores más pequeños.

Esta investigación muestra claras lagunas en las acciones que realizan los padres con los hijos y, sobre todo, en la efectividad de su intervención y medidas que toman con sus hijos e hijas para protegerles de los riesgos derivados del uso de Internet.

2.3 EU Kids Online III (2011-2014)

EU Kids Online I (2006 – 2009) identificó y evaluó críticamente los resultados de aproximadamente 400 investigaciones realizadas en el conjunto de países participantes, extrayendo las conclusiones, metodologías y políticas más relevantes. En la segunda fase (2009 – 2011) tuvo como objetivo prioritario obtener información

detallada y rigurosa sobre el uso de Internet, experiencias de riesgos y mediación para la seguridad de niños y niñas de 25 países europeos.

La tercera edición de EU Kids Online aún no ha presentado el informe de evaluación y análisis de EU Kids Online, pero si tenemos la oportunidad de acceder a algunos resultados comparativos entre el año 2010 y el 2014. Por otro lado, disponemos del informe del último periodo que nos deja información relevante sobre los objetivos y estrategias tomadas, a fin de conocer la evolución de los riesgos y de los nuevos usos de las TIC que afectan a los niños de toda Europa y que definen las áreas prioritarias que deben ser atendidas para su seguridad.

La red temática de EU Kids Online en este periodo 2011 – 2014 ha estado formada por 33 países que han formado parte del estudio:

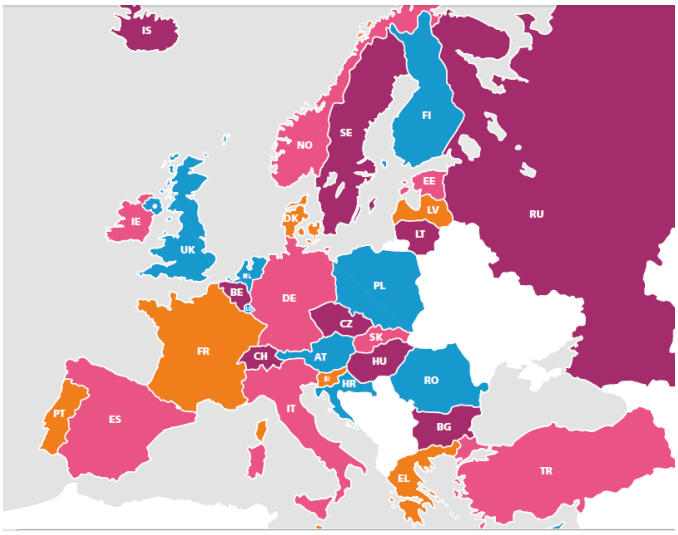


Figura 18 Países participantes en EU Kids Online III

(Grupo de Investigación EU Kids Online)

Medidas empleadas para la satisfacción de los objetivos

EU Kids Online III, ha desarrollado 6 áreas fundamentales para satisfacer sus objetivos:

- Gestión y evaluación de proyectos
- Base de evidencias europeas
- Hipótesis y comparaciones
- Significados de riesgo para los niños
- Difusión de los resultados del proyecto
- Recomendaciones de políticas

➢ Gestión y evaluación de proyectos:

Establecer procedimientos eficaces y flexibles que permitan la supervisión, evaluación y control de calidad para asegurar que se cumplan los plazos y normas de calidad.

Estimular nuevas investigaciones y facilitar la interacción y el contacto en la red de investigación iniciada.

➢ Base de evidencias europeas:

Codificar la información obtenida en cada país europeo y compartirla en una base de datos pública on line.

Evaluar el rigor científico de las pruebas obtenidas en los estudios realizados.

Reflexionar sobre las metodologías empleadas en las investigaciones sobre el uso de Internet seguro para los niños.

- Hipótesis y comparaciones:

Probar hipótesis y hacer comparaciones en el conjunto de datos de EU Kids Online II (Por ejemplo: analizar comparativas regionales) y escribir artículos o informes breves de los resultados obtenidos.

Obtener informes de comparaciones realizadas entre los resultados europeos y otras investigaciones simulares, por ejemplo en Rusia o Estados Unidos.

Investigar y realizar informes sobre comparaciones realizadas entre EU Kids Online y otras investigaciones temporales, como SAFT o Eurobarometer, para entender tendencias en el tiempo y cambios o evoluciones.

- Significados de riesgo para los niños

Identificar y estimular el uso de métodos cualitativos innovadores para explorar el contexto y las cuestiones éticas de las respuestas que tienen los menores a los riesgos.

Explorar lo que entienden los niños por riesgo.

- Difusión de los resultados del proyecto

Difundir los resultados obtenidos y estimular el estudio de los riesgos de los menores en Internet.

Difundir los resultados del proyecto entre los países miembros, maximizando la importancia de la investigación y apoyar la creación de políticas basadas en la evidencia.

- Recomendaciones de políticas

Supervisar y estar al tanto de los últimos debates e informaciones sobre políticas de seguridad en Internet.

Formular recomendaciones políticas basadas en resultados de los estudios realizados por EU Kids Online.

Evaluar las respuestas políticas procedentes de las propuestas salientes de EU Kids Online.

Contribuir al debate político a nivel europeo e internacional.

EU Kids Online III llamado 'A Thematic Network to Stimulate and Coordinate Investigation into the Use of New Media by Children'

En este periodo, el informe perteneciente a EU Kids Online III llamado 'A Thematic Network to Stimulate and Coordinate Investigation into the Use of New Media by Children', correspondiente al periodo desde Noviembre 2013 a Diciembre y coordinado por Sonia Livingstone y Leslie Haddon, nos muestra sus hitos prioritarios:

La red ha ampliado su labor mediante la inclusión de todos los Estados miembros, realizando comparaciones internacionales con los resultados obtenidos en países fuera de la CE y ampliando su participación con los actores políticos y las iniciativas de seguridad en Internet.

Se ha profundizado en los datos existentes europeos para obtener información que permita reforzar los conocimientos sobre el entorno del riesgo y las estrategias de mediación en la seguridad de los niños. Se han probado nuevas e innovadoras metodologías de investigación que nos permitan entender la naturaleza, significado y consecuencias de los factores de riesgo de las experiencias on line de los menores.

Por último, se ha actualizado la información on line de los resultados disponibles de las investigaciones existentes que aportan conocimientos sobre cuestiones nuevas y emergentes – por ejemplo, redes sociales, plataformas móviles, privacidad, protección de datos personales, seguridad y las prácticas de sensibilización en las escuelas, la alfabetización digital y la ciudadanía, servicios de geolocalización, etc.

Comparativa 2010/2014

Se han obtenido algunas conclusiones extraídas del informe "EU Kids Online: findings, methods and recommedations" (2014) en los que se realiza una comparativa entre los datos obtenidos más recientemente y los pertenecientes a las investigaciones de 2010. De los jóvenes europeos entre los 11 y los 16 años, se obtienen los siguientes resultados entre 2010 y 2014 respectivamente:

Están más expuestos a mensajes hirientes, aumentando del 13% al 20% los jóvenes que han recibido mensajes de este tipo.

Más jóvenes han visitado páginas pro-anorexia pasando de un 9% al 13%.

Han pasado del 7% al 11% los jóvenes que han visitado webs con contenidos sobre la autolesión.

Ha aumentado el ciberbullying, pasando de experimentarlo un 7% al 12% de los jóvenes.

Han aumentado los menores que afirman haber sido ofendidos de algún modo en la red, pasando de un 13% al 17% de los menores.

Han contactado con desconocidos a través de la red 32% - 29%

El porcentaje de menores que han visto imágenes con contenido sexual aumenta del 15% al 17%

Han recibido mensajes con contenido sexual 14% - 12%

Han visitado páginas web donde unas personas atacan a otras personas o colectivos, de manera ofensiva 13% - 20%

Han visitado páginas pro-anorexia o pro-bulimia 9% - 13 %

El resto de resultados que puedan resultar pertinentes para la investigación serán utilizados en la comparativa con los resultados de nuestra investigación.

¿Qué es lo que más molesta a los jóvenes?

La pornografía

Contenidos violentos, agresivos o del género gore.

La violencia real, o que parezca real, y la violencia contra niños y animales.

Los niños ven vídeos compartidos con los contenidos mencionados u otros riesgos.

Los niños expresan más preocupación por la violencia que las niñas, mientras que las niñas están más preocupadas con los riesgos relacionados con los contactos on line.

A los más pequeños les preocupa, principalmente, los riesgos relacionados con los contenidos y según van creciendo aumenta con ello la preocupación los riegos relativos a la conducta.

¿Qué formas de mediación parental son utilizadas por los padres y madres?

Hablar activamente con el joven sobre Internet, sus oportunidades y experiencia. Sentarte con el menor, y compartir actividades on line.

Aportarles estrategias para estar seguros en Internet.

Establecer reglas y restricciones sobre el uso de Internet.

Usar filtros y software de control parental, o utilizar algunas estrategia para monitorear las actividades de los niños.

En el informe se asocian beneficios a cada una de las acciones:

En el primer caso, se consideraría que las probabilidades de sufrir daños o exponerse a riesgos del menor son bajas y maximizaría las oportunidades y destrezas digitales del joven.

La segunda opción se puede utilizar con jóvenes que ya han tenidos experiencias de riesgo en Internet, para evitar otros futuros problemas.

La tercera de las opciones se asocia con baja probabilidad de daño, pero también bajas opciones de disfrutar oportunidades y aumentar sus destrezas digitales.

La última de las opciones no ha demostrado reducir los riesgos a los que se expone el joven.

Conclusiones generales

Los niños cuanto más utilizan Internet adquieren mayores habilidades digitales, lo que se traduce en poderse aprovechar de más oportunidades y, por lo tanto, mayores beneficios.

Como ya sabemos, no todos los efectos derivados de Internet son beneficiosos. La ganancia que obtiene un menor de Internet depende de su edad, género, estatus socioeconómico, apoyo familiar y del contenido positivo que tenga a su disposición.

El uso que hacen de Internet los niños está asociado a sus habilidades y oportunidades pero también a los riesgos existentes cuando están conectados. Es decir, cuanto más utilizan Internet, adquirirán mayores habilidades y aumentarán sus oportunidades en la red, pero también aumentará su probabilidad de exponerse a riesgos y, por lo tanto, de sufrir algún daño. Esta situación requiere un mayor esfuerzo para prevenir la exposición y el daño.

La exposición a riesgos no se traduce en daño recibido, sino que esto dependerá de su edad, género, estatus socioeconómico, su capacidad de recuperación y sus recursos para hacer frente a lo que experimenta en Internet.

También juegan un papel importante los padres, el centro educativo, sus compañeros, las normas reguladoras de la red, la provisión de contenidos adaptados por edades, los valores culturales y el sistema educativo. En este sentido, en el centro educativo los docentes pueden detectar conductas irresponsables en el uso de las TIC que puedan exponer a los riesgos derivados del uso de las TIC, sin embargo, para ello, las funciones docentes deben expandirse con independencia de las materias que se impartan. Como afirma Engracia Alda de la Fuente et al. (1998) "no existe un acuerdo al definir todas las funciones que deben asumir el docente y la escuela en el siglo XXI", aunque resulta innegable que las TIC están presentes en las aulas y en las vidas de los jóvenes, por lo que el docente debe asumir la detección de problemáticas relacionadas con las TIC, permitiendo anticiparnos a que la exposición a los riesgos puedan afectar negativamente a los jóvenes.

2.4 La industria en internet: Coalición CEO

Hacer frente a los riesgos procedentes del uso de Internet y de las TIC requiere de la implicación de todos los actores involucrados, desde las políticas gubernamentales a las empresas creadoras del software que se utiliza a través de la red.

Los beneficios que se obtienen de la creación de un "Internet seguro para los jóvenes" se han hecho visibles también para la empresas que, ante las presiones políticas y la ventajosa apertura de un mercado dirigido a los más jóvenes, han decidido

participar en la creación de una alianza que previsiblemente resultará beneficiosa para jóvenes, gobiernos e industria de Internet.

Coalición CEO 'hacer una mejor y más segura Internet para los niños y niñas"

El 1 de Diciembre de 2011, la Comisión Europea, dentro de la Agenda Digital, planteó dar un gran paso hacia un mundo digital libre de riesgos para los niños, mediante la formación de un coalición compuesta por las 28 empresas líderes en la industria, con el objetivo de "Hacer una Internet mejor y seguro para los niños y niñas" de todo el planeta (Comisión Europea, 2011). Las empresas co-fundadoras de la coalición fueron: Apple, BSkyB, BT, Dailymotion, Deutsche Telekom, Facebook, France Telecom-Orange, Google, Hyves, KPN, Liberty Global, LG Electronics, Mediaset, Microsoft, Netlog, Nintendo, Nokia, Opera Software, Research in Motion, RTL Group, Samsung, Sulake, Telefónica, TeliaSonera, Telenor Group, Tuenti, Vivendi, Vodafone.

Las primeras acciones de la coalición incluyen: facilitar la denuncia de contenidos perjudiciales; la configuración de privacidad adaptados a la edad del usuario y aumentar la oferta de opciones de control parental y filtros de seguridad.

La inclusión de las empresas desarrolladoras de bienes y servicios de Internet en la construcción de un mejor y más seguro Internet para los niños y niñas demuestra la importancia que dan en la Agenda Digital, y en propias empresas implicadas, a crear un Internet donde haya cabida para los niños sin que estén constantemente expuestos a los riesgos procedentes de la red. Al mismo tiempo que los padres y madres de los menores

puedan intervenir en la vida digital de sus hijos y utilizar herramientas disponibles para protegerles de estos peligros.

Neelie Kroes, vicepresidenta de la Comisión Europea, explicó como la coalición debe dotar, tanto a niños como a padres, de herramientas de protección transparentes y coherentes para hacer un mejor mundo en línea. Kroes afirma que las empresas participantes son líderes en seguridad on line de los niños y que juntos van a poder propiciar que la industria tenga objetivos comunes y así potenciar las oportunidades de Internet para los niños. (Comisión Europea, 2011)

El comunicado de la Comisión Europea en el que se informa de la creación de la coalición (2011) añade que los miembros de la coalición están de acuerdo en crear cinco áreas de atención:

Herramientas de denuncia de contactos y contenidos sencillas y sólidas, fáciles de manejar y accesibles desde cualquier dispositivo.

Configuración de privacidad adaptada por edades. Ajustes de configuración de privacidad que tengan en cuentas las necesidades de diferentes grupos de edad. Por ejemplo: en determinadas edades no sea posible exponer información personal a toda la red, si no únicamente a tus contactos directos.

Mayores posibilidades de la clasificación de contenidos que permita a los padres seleccionar grupos de edades.

Mayor número de opciones y mejor disponibilidad del control parental: herramientas sencillas que fomenten el uso de los padres y madres.

Acabar con los contenidos de abuso infantil. Mejorar la cooperación con la policía y líneas de ayuda para eliminar el material de abuso sexual infantil en Internet.

Para terminar, el comunicado referenciado añade que proporcionar seguridad a los menores cuando se conectan a Internet es un compromiso clave en la Agenda Digital europea.

EU Kids Online Y la Coalición CEO

Las primeras respuestas por parte de la comunidad científica internacional no se hicieron esperar y fue en Junio del 2012 que Sonia Livingstone, Kjartan Ólafsson, Brian O'Neill y Verónica Donoso publicaron el informe 'Towards a better Internet for children: findings and recommendations from EU Kids Online to inform the CEO coalition' con recomendaciones y sugerencias basadas en las conclusiones de las investigaciones que han realizado en los últimos años para hacer de Internet un lugar mejor y más seguro para los jóvenes.

El informe relaciona la información obtenida a través de los años de investigación de EU Kids Online con los objetivos de la coalición, presentando nuevos hallazgos que ayudan a establecer una línea base para el seguimiento del progreso.

El papel de los padres y madres es fundamental para satisfacer, especialmente, los cuatro primeros objetivos que se proponen en la coalición:

En el objetivo 1 pueden denunciar contenidos ilegales de Internet.

En el objetivo 2 deben de configurar las opciones de privacidad disponibles cuando sus hijos utilicen el software compartido y fomentar el uso de una configuración de privacidad adecuada para cada persona, en cada herramienta digital que se utilice.

En el objetivo 3 los padres son los encargados de supervisar el acceso a contenidos de sus hijos y trasmitirle la importancia de acceder únicamente a contenidos etiquetados que sean aptos para su edad.

En el objetivo 4 las herramientas de control parental deben de estar adaptadas a los riesgos que experimentan los jóvenes y han de conocer los intereses y preocupaciones de los padres, para que los padres valoren la utilidad y utilicen la herramienta.

En el estudio, se les pregunta si les preocupa que sus hijos sean contactados por desconocidos a través de Internet y que accedan a contenidos inapropiados a través de la red. El 33% y el 32% de los padres europeos encuestados muestran preocupación por estas situaciones de riesgos respectivamente.

Para crear iniciativas más efectivas, la coalición debe conocer los riesgos que se encuentran los jóvenes cuando están conectados a Internet. La Figura 19 nos muestra los riesgos que los jóvenes han experimentado cuando están conectados a Internet.

Para la obtención de los datos, han sido tenidos en cuenta los jóvenes de las edades especificadas que se han conectado a Internet en los 12 meses previos a la fecha en la que se les pasó los cuestionarios.

% who have	Age				All
	9-10	11-12	13-14	15-16	
Seen sexual images on websites*	5	8	16	25	14
Been sent nasty or hurtful messages on the internet*	3	5	6	8	6
Seen or received sexual messages on the internet*	n/a	7	13	22	15
Ever had contact on the internet with someone not met face-to-face before	13	20	32	46	30
Ever gone on to meet anyone face-to-face that first met on the internet	2	4	9	16	9
Come across one or more types of potentially harmful user-generated content*	n/a	12	22	29	21
Experienced one or more types of misuse of personal data*	n/a	7	10	11	9
Encountered one or more of the above	14	33	49	63	41
Acted in a nasty or hurtful way towards others on the internet*	1	2	3	5	3
Sent or posted a sexual message of any kind on the internet*	n/a	2	2	5	3
Done either of these	1	3	4	8	4

Figura 19 Riesgos que encuentran los jóvenes en Internet

(Livingstone S. H., 2011)

Si intentamos acercarnos a la evaluación de los daños que experimentan los jóvenes con éstos riesgos nos encontramos. Antes, debemos entender que al hablar de riesgo, nos referimos a que existe probabilidad de daño, no que necesariamente exista daño en el menor. Por otro lado, el daño puede ser leve o severo, estando íntimamente relacionado con el riesgo.

De los datos obtenidos en el estudio, podemos apreciar la relación entre la exposición a riesgos de los jóvenes con la percepción del daño del joven, por países. En

el caso de España, la exposición a los riesgos procedentes de Internet está por debajo de la media europea que se sitúa sobre el 40%, mientras que la española está alrededor del 35%. En cambio, respecto a los jóvenes que se han sentido molestos por la situación experimentada estamos por encima de la media europea.

Proporcionar herramientas eficaces de denuncia, ampliar las opciones de privacidad permitiendo adaptación por edades o clasificar los contenidos junto al control parental puede contribuir a reducir el riesgo, los daños y, en caso de darse el daño, incluso a recuperarse lo antes posible. Añadir que, "aparentemente" todo ello se alcanzarían sin limitar las ventajas que proporciona Internet para los jóvenes.

Recomendaciones e información a tener en cuenta en los objetivos de la Coalición

- **Herramientas de denuncia**

En la muestra tomada por EU Kids Online II se obtiene que el 13% de los jóvenes entre 9 y 16 años usan herramientas de denuncia cuando son molestados por algún riesgo en Internet. Si dividimos según los riesgos sufridos por los usuarios:

El 19% de las personas que han sido dañadas por recibir mensaje con contenido sexual.

El 15% de las personas dañadas por imágenes sexuales.

El 10% de las personas que han recibido contactos on line de personas desconocidas.

El 9% de las personas que han sufrido ciberbullying.

En este caso, no se tiene suficiente información para saber si el escaso número de jóvenes que denuncian o informan de daños sufridos cuando están conectados radica

en la falta de herramientas que permiten hacer esta tarea con facilidad, falta de conocimientos para realizarla, porque prefieran hablarlo con personas de referencia como padres y profesores o por falta de sensibilización sobre la importancia de las denuncias.

La Figura 20 nos muestra el porcentaje de satisfacción al utilizar una herramienta de denuncia. Los menores que han sido tenidos en cuenta en la Figura 20 son los que han experimentado alguno de los citados riesgos y usaron las herramientas disponibles para denunciar lo ocurrido.

% of those who used reporting tools who found it helpful, by type of online risk	%
Seen sexual images on websites	71[a]
Have been sent nasty or hurtful messages on the internet	61[a]
Seen or received sexual messages on the internet	64[a]
Ever met anyone face-to-face that first met on the internet	28[b]

Figura 20 Menores que usaron las herramientas de denuncia satisfactoriamente

(Livingstone S. H., 2011)

Se considera fundamental la implicación de la industria para la seguridad infantil on line. La diversidad de plataformas y dispositivos desde los que se conectan a Internet los menores son cada vez más diversos y deben existir herramientas sencillas y eficaces que les permitan denunciar los riesgos que se encuentran en la red.

Es evidente la baja participación de los menores en este fin por lo que se debe promover y sensibilizar sobre la importancia de la denuncia y, además:

Los niños deben conocer el funcionamiento y la utilidad de la herramienta.

Debe estar accesible en todo momento, no deben estar ocultas o en zonas de difícil acceso.

Todas las denuncias deben de obtener respuesta. El joven que denuncie un 'hecho' debe recibir feedback, viéndose de este modo la utilidad y garantía de "escucha".

Las herramientas deben ser abiertas y adaptadas a los riesgos cambiantes para que puedan ser reportados los riesgos conocidos y también los nuevos riesgos que surjan en la red.

Se debe permitir a cualquier persona, niño o adulto, que lo desee realizar una denuncia sin necesidad de crearse una cuenta en la aplicación en la que se ha detectado el riesgo. De éste modo se facilitará la denuncia.

Se debe conocer la existencia de organizaciones locales e internacionales que prestan ayuda y apoyo al usuario, así como las leyes que protegen sus derechos cuando están conectados.

Debe revisarse con prontitud los contenidos inapropiados o ilegales y/o las conductas delictivas y antisociales denunciadas.

Se debe conocer la eficacia del trabajo realizado, es decir, de los resultados obtenidos a través de las denuncias on line.

- **Configuración de privacidad**

El 38% de niños entre 9 y 12 años y el 77% de adolescentes entre 13 y 16 años, y el 59% de los menores en general, son propietarios de un perfil en una red social. En el caso de España, el 28% de niños entre 9 y 12 años, y el 81% de adolescentes entre 13 y 16 años, son propietarios de un perfil de red social.

Probablemente el lugar donde más información comparten los menores es a través de sus redes sociales, por este motivo debemos conocer como la protegen y así ver el valor que le dan a su información on line.

Si nos fijamos en la Figura 24 podemos ver el porcentaje de jóvenes que tienen su perfil en privado, público, parcialmente privado y los que desconocen cómo es el estado de su privacidad.

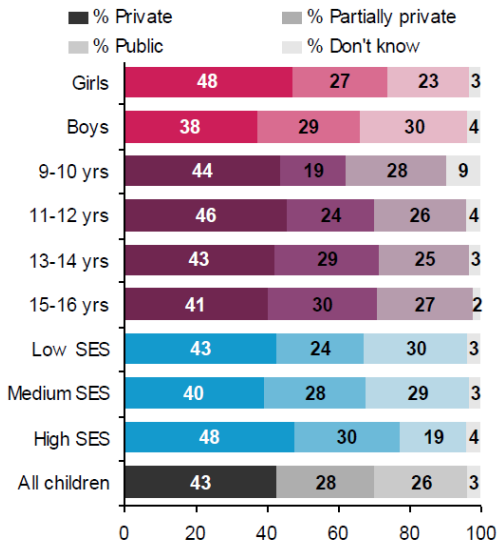


Figura 21 Uso de las herramientas de privacidad en las redes Sociales

(Livingstone S. H., 2011)

El 43% de los jóvenes tienen su perfil en privado, sólo sus amigos pueden verlo, mientras que el 28% comparten su información con amigos y amigos de amigos, al tenerlo parcialmente privado. El 26% comparten su información con toda la red y un 3% desconocen quien puede acceder a su información.

Verónica Donoso en su informe Assesment of the implementation of the Safer Social Networking Principles for the EU on 14 websites de 2011, se pregunta por qué

algunas personas usan la configuración de privacidad y otras no lo hacen, explicando que puede deberse a que prefieren utilizar la configuración por defecto, quizás porque es la recomendada por el sitio web. Cabría tener en cuenta que la configuración de privacidad de las redes sociales es pública por defecto.

En el informe se afirma que los niños son más propensos a tener un perfil público si no saben manejar adecuadamente la configuración de privacidad. Los conocimientos digitales suelen marcar la diferencia entre las personas que configuran según sus intereses su privacidad en las redes sociales y las que no lo hacen.

Las redes sociales son probablemente las aplicaciones usadas por más menores, sin embargo, para muchos de ellos aún sigue siendo complicado cambiar su configuración de privacidad, posiblemente porque utiliza un lenguaje que no entienden o porque desconozcan las diferencias de elegir una u otra de las opciones que te ofrecen. Teniendo en cuenta la edad de los menores, su situación de vulnerabilidad y sus habilidades digitales, el informe recomienda:

Los proveedores de los servicios de redes sociales deben facilitar en todo lo posible la modificación y configuración de sus perfiles a los menores de edad.

El usuario debe saber en todo momento que información es accesible para otros usuarios y qué usuarios pueden acceder a su información. El usuario debe tener el control sobre su información.

Se recomienda que para los usuarios más jóvenes se utilicen iconos intuitivos y pictogramas.

Los proveedores de servicios de Internet están en una posición privilegiada para promover la importancia de la seguridad en Internet y apoyar el trabajo desarrollado por los centros nacionales de seguridad en Internet.

Los usuarios más jóvenes deben poder utilizar herramientas más simples y adaptadas a sus necesidades, con tutoriales activados de manera predeterminada, y que faciliten el control de la herramienta.

Los servicios de Internet utilizados por los niños deben de evaluarse y ser transparentes con el fin de incrementar la confianza, el tratamiento de la seguridad, de la privacidad y de su configuración.

La información personal de los niños debe tener el máximo nivel de protección de la información, velando, por encima de todo, por los intereses de los menores.

- **Clasificación de contenidos**

Gentile (2011) obtuvo que las clasificaciones de contenidos por edades sólo son útiles si los padres están de acuerdo con ellas. Los padres, sin embargo, suelen estar en desacuerdo sobre las edades recomendadas para determinados contenidos, prefiriendo información detallada sobre el contenido que clasificaciones basadas en la edad.

El ratio de edad es considerado demasiado general al existir diferentes patrones culturales e ideologías que interfieren en la idea de proporcionar la edad recomendada para visualizar unos contenidos concretos o para acceder a determinada información. Es más recomendable aportar información breve, pero precisa, sobre el tipo de información que contiene el sitio web al que se va a acceder. De este modo, los padres podrán elegir

por ellos mismos la información a la que pueden acceder sus hijos, sin que interfiera en sus valores culturales, familiares y/o educativos.

- **Control parental**

Los resultados de los estudios SIP-BENCH I y II (2010-2012) muestran que la eficacia de los controles parentales es variable y depende del tipo de plataforma donde se utilicen. Por ejemplo, las herramientas de control parental utilizadas en los ordenadores personales son eficaces, mientras que cuando se evalúan las basadas en la web los resultados de los estudios realizados revelan que son ineficaces para los contenidos generados por el usuario, exceptuando el bloqueo de sitios web enteros. En cuanto al contenido para adultos, los resultados son más positivos que cuando se evalúan los contenidos inapropiados o perjudiciales. En este caso, el software se basa en palabras claves o listas negras.

El "control parental" es un tema bastante controvertido en la que no existe un claro consenso entre los expertos en seguridad en Internet. EU Kids Online, en la revisión de este informe, recomienda sustituir el "control" por la "mediación" aunque advierte que no tiene información relevante sobre los efectos de los "controles parentales" existentes. Aun así, recomienda realizar tareas de acompañamiento en el aprendizaje y acceso a la red, en vez de centrarse en la restricción de las actividades en línea, y recuerda la importancia de que estas herramientas respeten los derechos de los niños. Por último, se recomienda que en términos de diseño de las aplicaciones, estas herramientas sean fáciles de usar, instalar y configurar para garantizar que la experiencia del usuario sea óptima.

Coalición CEO 2013 – 2015

En la revisión presentada por la coalición a la Comisión Europea el 4 de Junio de 2013 en la revisión de los resultados conseguidos en 2012 y que continuaron trabajando en ellos en 2013 confirman que:

Los 31 miembros que forman parte de la coalición proporcionan herramientas de control parental y/o ajustes adaptados a la edad del usuario.

Se ha establecido a nivel europeo una base de datos de configuración de privacidad adaptada por edades que supone un portal para padres y educadores.

Se ha acelerado el desarrollo de medidas relacionadas con la seguridad de niños en Internet y ha aumentado el nivel de conciencia sobre la importancia que tiene.

Se ha creado una prueba piloto sobre calificación de contenidos generados por el usuario, en cooperación con organismo de calificación de contenidos.

Se han desarrollado rápidamente herramientas de denuncia en plataformas y aplicaciones.

Gracias a la coalición CEO, se ha mejorado la cooperación entre empresas con el objetivo de aprender unas de otras.

Creación de vínculos de trabajo técnico sobre la interoperabilidad con el fin de crear etiquetas de clasificación disponibles dentro y fuera de Europa y continuar desarrollando más herramientas innovadoras de información de usuario y software de filtrado de contenidos.

El informe presentado añade que el impacto de sus actividades se verá en los productos y servicios creados por los miembros de la coalición al final del año.

Iniciativas exitosas

Se han creado dos iniciativas especialmente interesantes que fueron presentadas a la Comisión Europea en los informes de progreso de 2014 de la CEO Coalition (Comisión Europea, 2014)

Clasificación de contenido

Se ha creado una herramienta para la clasificación de contenidos generados por el usuario que puede ser introducida en cualquier sitio web que permita subir vídeos, permitiendo aportar información del contenido del vídeo sobre 6 áreas: comportamientos, drogas, terror, lenguaje, sexo y violencia.

De este modo los espectadores podrán conocer el contenido de los vídeos antes de visualizarlos, pudiendo ser denunciado el vídeo por cualquier persona. La herramienta permite que desarrolladores o personas que visualicen el vídeo aporten información sobre su contenido, partiendo de un conjunto de preguntas elaboradas sobre las áreas mencionadas, que pueden ser modificadas y adaptarse a las realidades sociales y culturales de cada país o ciudad, siguiendo los criterios de calificación que se consideren más positivos.

La propuesta ha sido apoyada por la NICAM, Instituto Holandés de Clasificación de Medios Audiovisuales, cuyo comité está formado está formado por expertos en educación, en medios audiovisuales y en bienestar entre otros. Cuenta con más de 2200 empresas afiliadas (NICAM, 2013) y la BBFC, Consejo Británico de clasificación de películas, entidad británica sin ánimo de lucro encargada de la clasificación de vídeos y películas (BBFC, 1998).

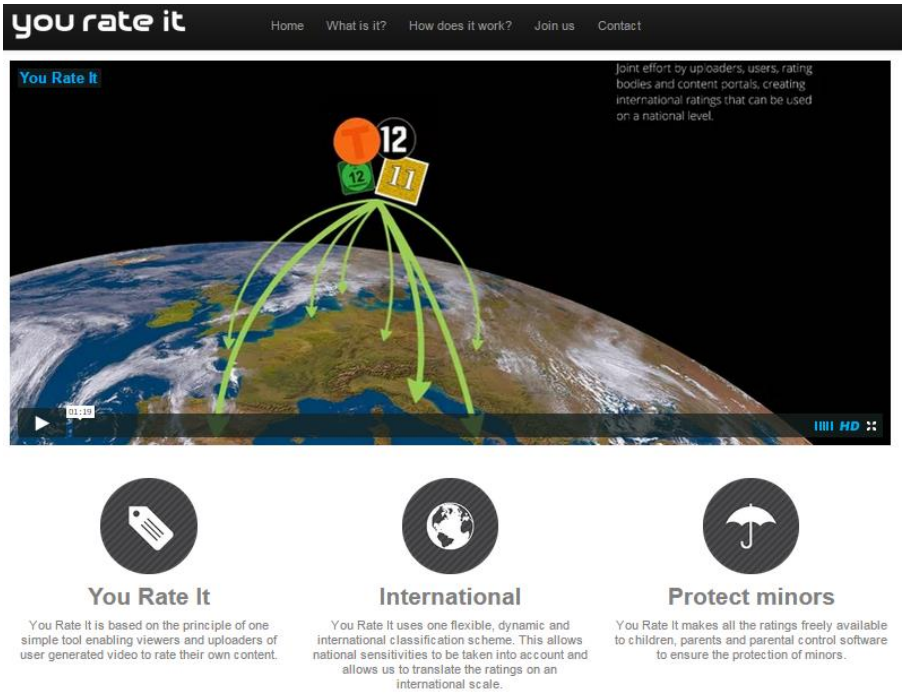


Figura 22 Herramienta You Rate It

(NICAM y bbfc)

La herramienta que puede solicitarse a través de la página web http://www.yourateit.eu/ acepta a través de su página web sugerencias que adapten la herramienta a las realidades del cada país.

Creación de la comunidad W3C

Se ha creado una comunidad, en la que se puede participar libremente, con el propósito de crear un modelo de datos neutral para crear etiquetas y descriptores de contenidos. Explican, además, que el modelo de datos incluirá categorías y campos consensuados que contengan información específica. Pretenden apoyarse en modelos de datos de clasificación de edad existentes.

Cualquier persona que lo desee puede formar parte del grupo rellenando un simple cuestionario, pudiendo compartir opiniones con para la creación de descriptores de contenidos con responsables de la BBFC, FSM, PEGI SA, Comisión Europea, etc.

El grupo no tardó mucho en dar resultados, publicando el primer borrador en Octubre del 2014 (W3C Group, 2013)

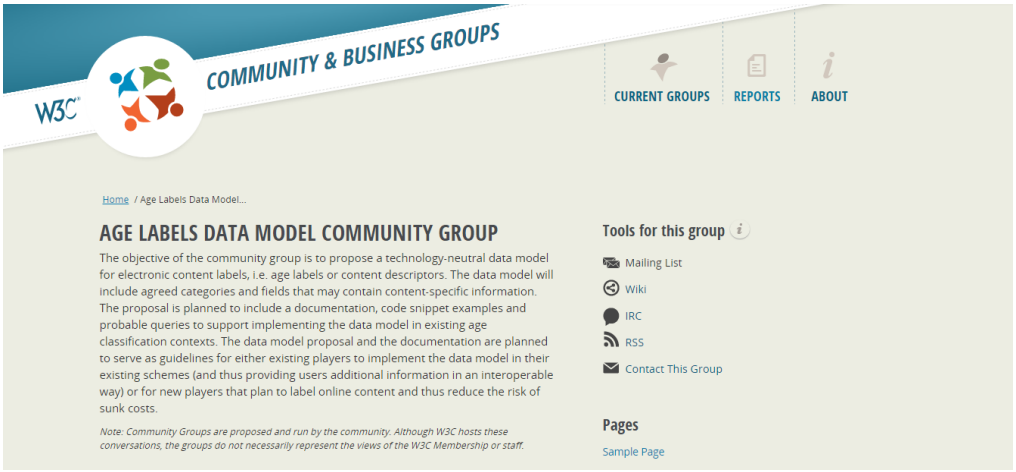


Figura 23 Herramienta You Rate It

(W3C Group, 2013)

Otros avances de la Coalición CEO

Además de todo lo mencionado hasta ahora, cada una de las empresas participantes han tenido en cuenta, supuestamente, los objetivos de la coalición y han desarrollado su software, plataformas o dispositivos de manera coherente con ellos.

A través de las páginas web que contienen información sobre la coalición, podemos acceder a los informes de las empresas implicadas en los que nos cuentas los avances obtenidos en consonancia con los objetivos de la coalición. A continuación, vamos a analizar brevemente el informe publicado por Apple y Samsung:

Apple

Según el informe aportado por la empresa Estadounidense (Apple Inc., 2014) la App Store ha incluido una categoría de niños que permite a padres y profesorado conocer que aplicaciones son adecuadas para el uso y disfrute de los menores. App Store también ha dado la posibilidad a los desarrolladores de su software de poder revisar las aplicaciones creadas para que cumplan los parámetros exigidos en la categoría de niños. Entre otras características, las aplicaciones deben contener unas políticas de privacidad concretas y no pueden contener publicidad comportamental. Además, las aplicaciones dirigidas a menores de 13 años deben contener el consentimiento de los padres para poder utilizarlas.

Apple ha proporcionado guías de control parental y ha creado tarjetas de regalo o asignación económica mensual para los padres que deseen dejar consumir a sus hijos recursos no gratuitos, controlando de este modo el gasto que les producen.

Por último, se han ampliado las opciones de control parental existentes, incluyendo a partir de 2013 el filtrado de sitios web a través de su navegador web Safari.

Samsung

En 2011, Samsung Electronics ofreció control parental que sus clientes se pudieron descargar para utilizarlos en sus dispositivos móviles. En 2012 también incluyeron software de protección a la infancia en sus SmartTv y continuaron desarrollando el software para sus dispositivos móviles (Samsung Electronics, 2013). En 2013, sacaron la Tableta *Samsung Galaxy Tab 3 Kids* para niños con control parental

de fábrica y software adaptado para niños, que les permite tener experiencias sanas y positivas a los menores (Samsung Electronics, 2013) .

2.5 Net Children Go Mobile

Net Children Go Mobile es un proyecto a través de 9 países (Bélgica, Dinamarca, Italia, Rumanía, Reino Unido, Alemania, Irlanda, Portugal y España) que tiene como objetivo investigar, a través de métodos cuantitativos y cualitativos, como las condiciones de uso y acceso a Internet a través de Smartphones, Tablet y otros dispositivos móviles se popularizan. Además, se plantea como todo ello afecta a la seguridad en Internet de los menores, tanto positiva como negativamente (Mascheroni & Cuman, 2014).

Para ello, se ha entrevistado a un total de 3565 menores de entre 9-16 años usuarios de Internet, padres de menores comprendidos entre dichas edades, profesores de educación primaria y secundaria y educadores de los diferentes países.

La siguiente información ha sido extraída del citado informe realizado por Giovanna Mascheroni & Andrea Cuman llamado *Net Children Go Mobile: Final Report*.

Uso de Smartphone y Tablet

En los últimos años, la manera de conectarse a Internet está cambiando con la popularización de los dispositivos móviles. El acceso a Internet se produce desde más lugares y pasamos más tiempo diario conectados. Los dispositivos móviles con conexión a Internet, refiriéndonos a los teléfono inteligentes o Smartphones y a las

Tablets, nos proporcionan una mayor autonomía en las actividades on line, además de una mayor portabilidad e individualidad, lo que a su vez, dificulta la supervisión paterna del uso de Internet de los menores.

Cabe decir, que, a pesar de la facilidad en la movilidad de los dispositivos móviles, el hogar sigue siendo el lugar donde los menores siguen realizando la mayor parte de sus conexiones. Además, el uso de dichos dispositivos no supone necesariamente su propiedad, ya que, especialmente los más pequeños, comparten los Smartphone con sus padres y/o hermanos, mientras que las Tablets suele ser un dispositivo de uso familiar de uso compartido.

Por otro lado, se observa que a pesar que los dispositivos móviles se basan en el principio de "en cualquier lugar, en cualquier momento", dicho precepto se ve limitado por restricciones sociales, técnicas y principalmente económicas. El informe detecta la necesidad de proporcionar conexión gratuita en centros educativos, a través de redes públicas proporcionadas por los gobiernos, etc., para fomentar la igualdad de oportunidades de acceso y, en el caso de los colegios, beneficiarse del uso de Internet durante sus clases. Por último, anima a los operadores a mostrar una mayor transparencia en sus tarifas de Internet y a la creación de herramientas y Apps que permitan a los usuarios controlar y conocer sus facturas de manera cómoda y fiable.

Coincidiendo con la llegada de los Smartphones y Tablets, los menores empiezan a usar Internet y dispositivos móviles cada vez a edades más tempranas. La media de edad de iniciación depende de cada país, pero en todos coincide que dicha iniciación en el uso de Internet es varios años previa a obtener un Smartphone propio.

Una de las preguntas que más debate genera entre padres, es cuál es la edad apropiada para que los menores tengan su primer dispositivo móvil. El momento suele coincidir con la llegada de un cumpleaños, Navidad o por haber cumplido con un objetivo previamente establecido, como 'sacar buenas notas'. Curiosamente, el Smartphone, no siempre llega a petición del menor, sino como regalo inesperado por parte de los padres. Dicho regalo puede responder a una necesidad de control o para favorecer la autonomía e inclusión social de sus hijos.

Cambios y consecuencias

Los datos obtenidos de la investigación muestran que la comunicación, el entretenimiento y el uso de Internet para el colegio encabezan la lista de actividades diarias realizadas on line. Compartir (imágenes, videos, documentos), las redes sociales y el ocio a través de Internet son las actividades que más se han visto incrementadas en los últimos años.

Los jóvenes utilizan las redes sociales de un modo natural en diferentes ámbitos de su vida (Gómez García, Ruiz y Sánchez, 2015b). Sin embargo, aunque los menores cada vez están más involucrados en actividades on line, no todos los grupos de edad se benefician por igual de sus ventajas. También existen notables diferencias entre los países de habla inglesa y el resto de nacionalidades, dada la existencia de mayor material adaptado a las necesidades de los menores en este idioma. Por todo ello, los gobiernos y desde la coalición CEO a toda la industria, se debe promover la necesidad de adaptar a los países de habla no inglesa los materiales, así como de crear más materiales adaptados a las características de cada país.

Cabe señalar que el uso de los dispositivos móviles no ha desterrado a tecnologías previas, pues son muchos los menores que afirman que siguen prefiriendo el PC para actividades como ver videos, hacer los deberes o jugar a videojuegos. Esto puede deberse, en el caso de los videojuegos, a la necesidades de mayores requerimientos técnicos de muchos videojuegos, que los existentes en Smartphones y la mayoría de las Tablets, o por comodidad visual para hacer deberes, ver vídeos o también jugar a videojuegos.

Sin embargo, los Smartphones se sitúan como los preferidos para las comunicaciones. La facilidad en su movilidad, las tarifas planas disponibles, la gratuidad para conectarse a Internet desde algunos lugares y la comunicación simultánea con múltiples usuarios, son algunos de los motivos que exponen los jóvenes en su preferencia. Son muchos los que afirman sentirse más sociables desde que tienen Smartphone.

En cuanto a las redes sociales, más del 68% de los jóvenes afirman tener, al menos, un perfil en una red social. Además, muchos combinan diferentes perfiles en diferentes redes sociales usando cada una de ellas para diferentes fines o públicos. Dicha práctica promueve el desarrollo de sofisticados repertorios de prácticas, dispositivos y servicios entre los que elegir el más apropiado a cada situación. Facebook sigue siendo la Red Social líder en todos los países, géneros y grupos de edad.

Asimismo, se observa que con la adquisición y desarrollo de las habilidades digitales los menores se vuelven más sensibles sobre la información que ofrecen de sí mismos a través de la red. Curiosamente, muchos de los jóvenes que manejan su

información de manera recelosa manejan paralelamente un perfil público con uno privado dentro de una misma red social.

En los últimos cuatro se observa un importante desarrollo de las habilidades digitales que permite a los menores navegar en Internet de manera segura. El incremento de estas habilidades es sustancialmente mayor en los menores que usan dispositivos móviles, frente a aquellos que no los usan de manera habitual.

Por otro lado, los menores conocen el modo de proteger un dispositivo móvil con clave de acceso, desactivar las funciones de localización o encontrar información sobre cómo utilizar de manera segura un Smartphones/Tablet. Además, más del 58% de los entrevistados consideran tienes más conocimientos que sus padres sobre el uso de Smartphones y Tablets.

Sin embargo, son muchos los menores (especialmente en los grupos de menor edad) que aún tienen carencias en las habilidades que permiten un uso seguro de Internet. Es por ello, que el Net Children Go Mobile recomienda a los centros educativos incluir en su currículo educación específica para el uso seguro de los dispositivos móviles.

Por último, añadir que aunque son muchos los efectos beneficiosos que la comunicación móvil ha traído consigo, también existen consecuencias negativas: sobre-dependencia, perpetua apatía, vínculo de entretenimiento-móvil, estar siempre conectado, malinterpretaciones en la comunicación o exclusión por parte de los iguales. Para paliar estas consecuencias negativas es recomendable promover las interacciones cara a cara y un uso responsable de los dispositivos móviles.

Algunas de las recomendaciones propuestas por parte de la investigación al respecto son el empoderamiento de los menores por parte de los padres para un uso responsable de los dispositivos móviles y la comunicación on line. Además, proponen a la industria la posibilidad deshabilitar por defecto las notificaciones para los menores de edad.

Riesgos

Más del 17% de los menores afirman haber experimentado en Internet alguna situación que les haya molestado o preocupado. Existen diferencias significativas respecto a género y edad: chicas (21%) y grupos de menores de mayor edad (23%). También hay diferencias destacables en cuanto a la hora de informar a terceros que algo está incomodándoles a través de Internet: los daneses encabezan la lista con un 39%, mientras que los italianos se sitúan en la cola con un 6%.

La exposición a los riesgos se incrementa con la edad y un mayor uso de los dispositivos móviles. Desde EU Kids Online, hemos podido apreciar que a mayor uso, mayor riesgo. Como hemos visto con anterioridad, el mayor uso que los menores hacen de Internet implica la intensificación de medidas para evitar que se expongan a riesgos, como: medidas políticas que hagan Internet una experiencia segura para los menores europeos, contenidos adaptados, mayor y más temprana mediación parental en el entorno digital, etc.

Bullying (on and off line)

El nivel de acoso escolar se ha visto incrementado notablemente de 2010 a 2013-2014. Este incremento está asociado a las nuevas comunicaciones y las oportunidades

que éstas ofrecen. Algunos menores consideran que los dispositivos móviles facilitan el ciberbullying, ya que permiten permanecer constantemente conectados y disponibles. Los colegios deben jugar un papel importante a la hora de prevenir estas situaciones, ya que la mayor parte ocurren entre compañeros de clase.

Las características de la red facilitan el acoso gracias a la distancia que genera y a la eliminación de la presión del 'cara a cara', propiciando que jóvenes acosen a otros jóvenes a través de Internet que no lo harían cara a cara. Además, es habitual que los compañeros de clase compartan números de teléfonos sin permiso del propietario, lo que, junto con los nuevos modelos de comunicación, permite una interacción anónima facilitadora del acoso on line. Estos motivos, unidos a la portabilidad de los dispositivos, simplifican que los jóvenes puedan perpetuar el acoso a las víctimas, aun estando fuera del centro escolar o haciendo otras actividades aparentemente lejos de las TIC.

Es necesario, en relación a este tema, una mayor concienciación a través de campañas educativas de la importancia de un uso responsable de los dispositivos móviles y sus aplicaciones.

Exposición de la privacidad y uso incorrecto de los datos personales

La exposición de datos personales es el origen de la mayor parte de los riesgos en la red. Agresiones, comunicación sexual y malversación de los datos están constantemente relacionadas. Se debe valorar adecuadamente nuestra información personal y ser conscientes de las implicaciones que tiene exponer nuestra información en la red o con nuestros contactos.

Compartir los dispositivos móviles con iguales o compañeros da acceso a éstos a nuestros datos personales, fotos o mensajes. Es importante hacer consciente de ello a los menores y promover un compartir responsable. Deben valorar adecuadamente las personas con las que comparten los teléfonos móviles ya que puede ser utilizado para dañarles.

Contenido sexual y comunicación

Los nuevos dispositivos y plataformas ofrecen nuevas opciones a los jóvenes para acceder y compartir contenidos sexuales. Sin embargo, los menores se declaran más preocupados por el riesgo del "sexting". Aunque la incidencia del sexting se ha visto disminuido desde 2010, sigue existiendo y continúa habiendo diferencias entre edades y género.

El revenge sexting, que consiste en el reenvío de imágenes o vídeos de carácter sexual de la ex pareja, a otras personas como venganza para hacerle daño, es una práctica habitual que está perseguida por la ley en España. Es necesario concienciar de las consecuencias que tienen este tipo de acciones desde los derechos digitales a campañas de igualdad y anti-sexismo.

Uso excesivo.

Muchos son los menores que espontáneamente mencionan su adicción o uso excesivo, y la gran mayoría están de acuerdo en que pasan demasiado tiempo on line y/o con sus Smartphone.

Los jóvenes perciben los Smartphone como una extensión de su cuerpo. Los Smartphones están tan integrados en nuestra cotidianidad que casi forman parte de

quienes somos. Como consecuencia, es entendible que los jóvenes se sientan incómodos cuando no pueden revisar su teléfono para comprobar si hay alguna novedad, ya que es un hábito que forma parte de sus rutinas.

Gran parte de los menores confiesan descubrirse haciendo cosas en el móvil que realmente no les interesa o pasan menos tiempo del que deberían con familiares, amigos o haciendo los deberes debido al uso continuado de los dispositivos móviles.

Enseñar a los menores a lidiar con la presión social y la dependencia es una de las recomendaciones que Net Children Go Mobile lanzan a ONGs, colegios y familias. Los menores deben comprender que es totalmente válido estar "off line" y aceptar que no es necesario contestar inmediatamente a todo mensaje o notificación.

Otros riesgos

Anuncios, spams y mensajes emergentes requieren de habilidades específicas, especialmente para lidiar con juegos o aplicaciones de pago que son de interés para los jóvenes.

Por último, más allá de los riesgos propios de la red, nos encontramos con los riesgos ligados al valor emocional al dispositivo en sí. Un miedo compartido por muchos menores de los diferentes países es el hecho que su Smartphones pueda sufrir algún daño o ser robado. La reacción observada en menores que pierden su móvil de manera inesperada en un shock emocional.

Son muchas las estrategias que los menores utilizan para lidiar con los riesgos expuestos, la mayoría suelen combinar más de una de las siguientes estrategias:

Estrategias autosuficientes empleadas especialmente para riesgos asociados a la localización, privacidad o uso excesivos de los dispositivos móviles

Medidas técnicas que incluyen la intervención o interacción con el dispositivo o el servicio para resolver el problema

Confrontación, referida a confrontaciones personales o discusiones cara a cara u on line.

Cooperación/colaboración entre los menores tanto en términos de apoyo emocional como a nivel técnico, ayudándose entre iguales a resolver un determinado problema

Retiro o desvinculación del problema. Ante algunas situaciones los menores perciben que las estrategias disponibles van a ser inefectivas.

Por lo tanto, la comunicación es un modo común entre los menores de lidiar con las situaciones problemáticas en la red. Aunque uno de cada tres jóvenes dice no tener con quien hablar sobre sus preocupaciones o miedos de Internet. Las personas con quien los menores tienden a hablar sobre estas situaciones son sus madres (71%) amigos (57%) y sus padres (54%).

Mediación parental

La esfera familiar es un espacio social destacado que influye en las experiencias on line de los menores. Las estrategias adoptadas por los padres para regular el acceso y uso de sus hijos a Internet será un importante mediador a la hora de reducir los riesgos en las red. Los padres utilizan múltiples estrategias, entre las que se encuentran:

Mediación activa del uso de Internet con actividades como hablar sobre contenidos nocivos en Internet o compartiendo experiencias on line.

Mediación activa sobre la seguridad en la red, promoviendo usos seguros y responsables en Internet

Mediación restrictiva, limitando y regulando el tiempo de navegación, la localización o las actividades on line.

Restricciones técnicas mediante filtros, restricciones de acceso uso o monitorización de las actividades de los menores en la red.

Control o revisión del historial de actividad on line

La mayoría de las familias (68%) emplean al menos dos estrategias de mediación del uso de Internet de sus hijos. La más común es hablar con los menores sobre qué hacen cuando se conectan a Internet (66%) y estar junto a ellos mientras sus hijos están on line (58%). Estos tantos por cientos son aún más altos cuando se pregunta a los menores, en lugar de a sus padres.

Desde Net Children Go Mobile proponen un fomento de un entorno donde los menores aprendan poco a poco cómo lidiar con los riesgos de los dispositivos móviles. Las familias, más que nunca, necesitan hablar y compartir sobre sus experiencias on line y juntos poner en marcha estrategias que se perciban como ayuda y no como una intrusión. Además, sería importante el desarrollo de Apps seguras que promuevan un dialogo activo entre los menores y sus familias.

De la investigación se desprende que el acuerdo de normas es menos común que la mediación para el uso seguro de Internet de los menores. Si analizamos los datos por países, podemos observar como Bélgica, Irlanda y Portugal siguen un patrón de altas

restricciones y baja privación del uso de Internet. En el lado opuesto, se sitúa Dinamarca y Rumanía con una escasa regulación y un alto uso de Internet de los menores en sus propias habitaciones. Por último, Italia y Reino Unido mantienen patrones más restrictivos que la media, aunque los menores siguen haciendo un alto uso de Internet en sus habitaciones.

Las diferentes estrategias adoptadas por las familias persiguen, principalmente, la reducción de riesgos de sus hijos en la red, pero también suponen un límite a la privacidad de los mismos, por lo que las respuestas de los menores a dichas estrategias también son diversas: aceptación, no aceptación o intentar navegar al margen de las normas.

El colegio

Existen amplias diferencias entre países en cuanto al uso de Internet en los centros escolares, sus instalaciones digitales y la regulación del uso de los Smartphones.

Portugal y Dinamarca encabezan la lista de los países que más usan Internet diariamente en sus centros educativos, mientras que Italia se sitúa en el opuesto.

Más allá de las diferencias entre países, la infraestructura digital y la disponibilidad de acceso a Internet están fuertemente marcadas por la edad y el estatus socio económico. Los alumnos más jóvenes y los menores de clases socioeconómicas más bajas tienen un acceso diario notablemente inferior.

El 54% de los menores afirman que nos les está permitido usar Smartphones en el colegio, el 31% que les está permitido su uso con ciertas restricciones. Los profesores suelen ser flexibles, especialmente con los alumnos de los cursos más altos.

La mayoría de los menores, aunque comparten y entienden las normas y restricciones de uso de los Smartphones en los centros educativos, sienten la necesidad de revisar regularmente su móvil. Las medidas tomadas por los profesores son muy variadas, aunque la más común es la confiscación del dispositivo.

Sin embargo, sería importante promover un uso adecuado del móvil en las aulas, otorgándole fines educativos. Una de las propuestas derivadas de la investigación es la formación al profesorado para la inclusión de los dispositivos móviles en el aula con fines educativos. El profesorado debe ser capaz de utilizar, no sólo plataformas educativas tradicionales, sino de gestionar un entorno de aprendizaje aprovechando los beneficios de las herramientas en red (Ruiz, Sánchez y Gómez, 2013).

España

España, al igual que Alemania, sólo ha formado parte de la investigación cualitativa del estudio, por lo que son menos los datos obtenidos con respecto al resto de países participantes que también han sido tenidos en cuenta el estudio cuantitativo.

A continuación se presentan algunos de los datos cuantitativos derivados de otros estudios realizados en España.

El 70% de los hogares españoles cuentan con acceso Internet y el 65% de la población total (46.507.760 habitantes) son usuarios de Internet.

Internet está mucho más difundido entre los menores de 10-15 años 92.2% de los menores usan ordenadores y el 91.8% utilizan Internet. Además, el 63% de dichos menores tienen su propio PC. El porcentaje aumente gradualmente con la edad desde un 26.1% con 10 años, hasta 90.2% entre los menores de 15.

El 95.6% de los hogares españoles cuentan con al menos un teléfono móvil y el 86.8% de los individuos de más de 10 años son usuarios de los móviles.

Casi el 70% de los menores españoles de más de 12 años tiene un móvil y con menores a partir de 14 años ese tanto por ciento aumenta hasta el 83%. El 76% de los menores españoles entre 11 y 14 son usuarios de WhatsApp. Y, además, el 65% de los menores de ese mismo rango de edad participan en grupos de WhatsApp.

De los datos obtenidos, se desprende que el 23% de los jóvenes entre los 11 y los 14 años suben regularmente fotos/videos a Internet, el 52.2% juega habitualmente con dispositivos móviles y el 52% afirma pedir permiso a sus padres para instalar una nueva aplicación.

El uso de las TIC en los centros educativos

Según los datos desprendidos de la investigación "Estudio de las TIC en Educación" España, en los cursos más bajos, el números de alumnos por ordenador es más bajo que la media europea, situándose próximo al número en los países nórdicos. Como norma general, el número de alumnos por ordenador aumenta con la edad. Sin embargo, España se sitúa entre los países con menor ratio de pizarras digitales.

2.6 Agenda digital para Europa

El 19 de Mayo de 2010 la Comisión al Parlamento Europeo saca un comunicado titulado 'Agenda Digital para Europa'. En él, la Comisión Europea propone "una Agenda Digital para dirigir a Europa hacia un crecimiento inteligente sostenible e integrador" (Comisión Europea, 2010).

La Agenda Digital constituye uno de los siete pilares de la Estrategia Europea 2020, que establece un conjunto de objetivos para el crecimiento europeo. Por su parte, "la Agenda Digital propone explotar el potencial de las tecnologías de la información y la comunicación (TIC) con el fin de fomentar la innovación, el crecimiento económico y el progreso" (Comisión Europea, 2010).

El informe presentado por la Comisión Europea explica que "la finalidad genérica de la Agenda Digital (2010) es obtener los beneficios económicos y sociales sostenibles que pueden derivar de un mercado único digital basado en una Internet rápida y ultrarrápida y en unas aplicaciones interoperables". Posteriormente, explica que la Comisión Europea puso en marcha en marzo de ese mismo año la estrategia Europa 2020 con el objetivo de salir de la crisis y dejar a Europa en una situación ventajosa para la próxima década. La Agenda Digital es una de las siete iniciativas de la estrategia Europa 2020 y considera que la consecución de sus objetivos es fundamental para alcanzar los objetivos de la estrategia Europa 2020.

Contexto de las TIC en la Agenda Digital:

En 2010, el sector TIC genera el 5% del PIB de Europa, lo que se traduce en 660.000 millones de euros al año, pero contribuye mucho más al crecimiento de la productividad general, aproximadamente un 20% atribuible directamente al sector de las TIC y un 30% de las inversiones en TIC en otros sectores productivos. Las TIC permiten transformar el modo de funcionamiento de otros sectores, mejorando el proceso productivo y/o ahorrando costes, lo que ha facilitado su entrada en estos sectores. Las TIC han supuesto todo un fenómeno social, cambiando el estilo de vida

de los europeos que en 2010 ya eran más de 250 millones de personas las que usaban Internet a diario.

El desarrollo de las redes de alta velocidad ha tenido el mismo impacto revolucionario que tuvieron en su día las redes eléctricas y de transporte. Los servicios convergen y los que ayer se ofrecían en el mundo físico, hoy se ofrecen en el digital, suponiendo un cambio en nuestros hábitos de consumo.

Lejos de estancarse, las TIC no paran de evolucionar y adaptarse a las necesidades de los usuarios, proponiendo constantemente continuas mejoras. Los teléfonos móviles han dado paso a los teléfonos inteligentes y éstos a las Tabletas. Hoy en día, los grandes multinacionales luchan por encontrar el dispositivo que suponga la nueva revolución social. Ahora hablamos de relojes o gafas inteligentes, sin conocer el efecto que tendrá en el mercado europeo y mundial, pero sin duda nos ofrece un mensaje claro. La revolución digital, no ha hecho más que comenzar.

Sin embargo, el poder transformador de las TIC, todas las ventajas que ofrecen en el desarrollo empresarial y las oportunidades que pueden surgir a través de ellas, evidencian la necesidad inmediata de atención a las preocupaciones y limitaciones que genera: la privacidad y la seguridad en el entorno on line.

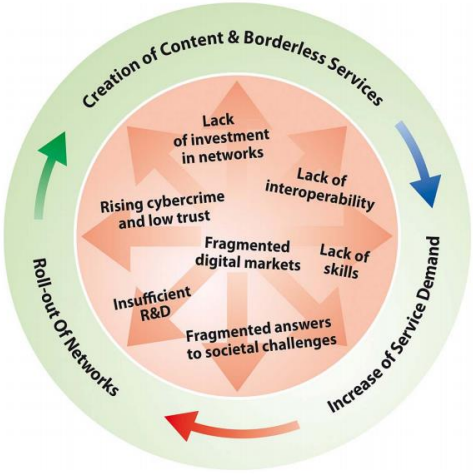


Figura 24 Ciclo virtuoso de la economía digital

La Figura 24 nos muestra el flujo de actividad que exige un entorno empresarial que fomente la inversión y el espíritu emprendedor.

Por otro lado, la población europea observa como el incremento y aceleración de los servicios y desarrollo de Internet, no se traduce en la prosperidad y crecimiento económico que se esperaba en Europa.

En la Declaración de Granada y en la Resolución del Parlamento Europeo, la Comisión ha confeccionado la lista de los siete obstáculos más importantes, que podemos ver representados en el interior de la Figura 24, justificando la necesidad de una respuesta política global y unificada a nivel europeo. Europa se está quedando a la zaga de sus socios industriales. Si comparamos, por ejemplo, la penetración de las redes de alta velocidad basadas en fibra óptica en Europa se situaba en un 1%, frente al 12% de Japón y al 15% de Corea del Sur. O el gasto en investigación y desarrollo de las TIC en Europa representaba el 40% del gasto estadounidense (Comisión Europea, 2010).

Áreas de actuación

La Agenda Digital en 2010 – 2014 ha tenido ocho campos de actuación:

- Un mercado único digital dinámico
- Interoperabilidad y normas
- Confianza y seguridad
- Acceso rápido y ultrarrápido a Internet.
- Investigación e innovación.
- Fomentar la alfabetización, la capacitación y la inclusión digitales.
- Beneficios que hacen posibles las TIC para la sociedad de la UE.
- Aspectos internacionales de la Agenda Digital

En nuestra investigación nos centraremos en el área que abarca la 'Confianza y Seguridad' y en sus elementos, relacionados directa o indirectamente con el objeto de estudio.

Confianza y Seguridad

Los europeos no adoptarán una tecnología en la que no confíen; la era digital no es ni el «Gran hermano» ni el «salvaje oeste cibernético» (Comisión Europea, 2010).

El tercero de los campos de actuación de la Agenda Digital (Confianza y Seguridad) visibiliza el valor y la importancia de la confianza y seguridad de población en los medios digitales.

Se ha explicado la importancia del desarrollo de las TIC en el motor económico europeo. Los esfuerzos y el buen hacer en esta materia no cumplirían los objetivos establecidos si los usuarios no se sienten seguros y protegidos cuando se conectan a Internet.

Por otro lado, el consumo a través de la red está lejos de aprovechar su potencial. Por ejemplo, si tenemos en cuenta las descargas musicales hasta 2010, en Estados Unidos se producen cuatro veces más descargas que en Europa. El informe nos dice que se debe a la falta de ofertas legales y a la fragmentación de los mercados.

Si se quiere fomentar el consumo de bienes o servicios a través de Internet, ya sea música, software o cualquier otro tipo de compra, en primer lugar se debe potenciar la seguridad que le ofrece el medio digital para realizarla. En caso de no existir esta confianza por parte del consumidor, los esfuerzos realizados para que la persona disponga de red de conexión a Internet en su localidad, ordenador personal o la oferta de las compañías que ofrecen los servicios de conexión a Internet a precios competitivos, perderían su potencial y capacidad de expansión al tener limitada su utilidad. La seguridad en los nuevos dispositivos y software deben ser intrínseca y deben ser plenamente fiables. En el informe, la Comisión Europea nos afirma que hasta el momento Internet ha demostrado ser segura, resistente y fiable, pero los usuarios finales continúan siendo vulnerables a una amplia gama de amenazas cambiantes. Un dato es que en los años anteriores al informe hay estimaciones que sugieren que entre el 80 y el 98% de los mensajes que circulan por la red, son mensajes no deseados. Los ataques son diversos y cada

vez más sofisticados, buscando constantemente la vulnerabilidad de los usuarios ya sea en los aspectos técnicos, de falta de conocimientos o inseguridad.

La Comisión Europea (2010) responsabiliza tanto a personas individuales como a entidades privadas y entidades públicas para hacer frente y neutralizar las amenazas derivadas de la red y reforzar la seguridad en la sociedad digital. Por ejemplo, "para combatir la explotación sexual y la pornografía infantil, pueden constituirse plataformas de alerta a nivel nacional y de la UE, junto con medidas encaminadas a suprimir los contenidos nocivos y evitar su visualización. También resultan esenciales las actividades educativas y las campañas de sensibilización para el público en general: la UE y los Estados miembros pueden redoblar sus esfuerzos, por ejemplo, a través del programa Safer Internet, para informar y formar a los niños y a las familias sobre la seguridad en línea, además de analizar el impacto que tiene sobre los niños el uso de las tecnologías digitales" (Comisión Europea, 2010). La industria también puede participar desarrollando y regulando el acceso a contenidos inapropiados de los menores o cuando los menores utilizan los servicios ofrecidos a través de Internet.

Tal como podemos observar, la implicación debe ser de todos los actores que intervienen en el proceso que lleva a los usuarios a situarse frente a un riesgo procedente de Internet.

Por otro lado, la ley debe proteger la intimidad y los datos personales de los usuarios, ya que constituye un derecho fundamental en la Unión Europea.

Es necesario que existan sistemas de denuncia eficaces que aporten al usuario de Internet tranquilidad y seguridad. El ciudadano debe conocer los métodos de denuncia y los equipos de emergencias informáticas, los CERT, y éstos han de cooperar con los organismos policiales y judiciales, para conseguir tiempos de respuesta aceptables. En el informe consideran imprescindible la cooperación entre los agentes pertinente a nivel mundial, para de manera eficaz para luchar contra las amenazas y reducirlas, dado la facilidad de acceso a páginas web con contenidos ubicados en cualquier parte del mundo. También proponen que se creen acciones conjuntas para la lucha contra la delincuencia informática, que cuente con el apoyo de la Agencia Europea de Seguridad de las Redes y de la Información, ENISA.

La Comisión Europea (2010) pretende crear medidas encaminadas a conseguir una política de seguridad en la red que incluyan iniciativas legislativas que permitan:

- Reaccionar con rapidez en caso de ciberataques.
- Una normativa sobre la jurisdicción en el ciberespacio antes de terminar.
- Establecer una plataforma europea de la ciberdelincuencia de Europol, en funcionamiento.
- Llevar acciones concretas contra la delincuencia informática y los ataques a la seguridad
- Acciones para la protección de los datos personales y de la intimidad.
- Fomentar el diálogo entre las partes implicadas en el uso y utilización de las redes sociales y fomentar la autorregulación de los proveedores de servicios

europeos y mundiales, especialmente en lo que se refiere al uso de las herramientas por menores.

- Etc.

Actualización de 'Una Agenda Digital para Europa'

La Agenda Digital europea fue revisada por la comisión en diciembre de 2012 con el objetivo de establecer medidas más específicas para generar crecimiento y empleo en Europa, en un momento en que la Comisión Europea determina que es necesario esforzarse más para reactivar el rendimiento económico de Europa viendo grandes posibilidades en la economía digital que crece a un ritmo siete veces superior al resto de la economía (Comité de las Regiones, 2013).

El 18 de Diciembre de 2012 la Comisión Europea emite un comunicado de prensa en el que expone las nuevas prioridades digitales para los años 2013 y 2014. En él, Neelie Kroes, Vicepresidenta de la Comisión Europea, declara "2013 será para la Agenda Digital un año aún más activo que los precedentes. Mis principales prioridades son aumentar la inversión en la banda ancha y maximizar la contribución del sector digital a la recuperación de Europa". (Comisión Europea, 2012b)

Podemos observar que las palabras de Kroes se centran en la recuperación económica a través de las tecnologías de la información y la comunicación. Ante estas palabras nos surge la pregunta: ¿cómo de importante es considerada la seguridad con la que los jóvenes se conectan a Internet en la recuperación económica a través de las TIC?

Repasando las prioridades digitales para los años 2013 y 2014, podemos ver que la seguridad en Internet sigue considerándose una parte importante puesta presente entre las nuevas prioridades de la Agenda Digital (2012):

Creación de un marco regulador de la banda ancha nuevo y estable.

Debido a la necesidad de mayor inversión privada, en 2013 se proponen diez medidas, entre ellas una nueva metodología de cálculo de costes para el acceso de mayoristas a las redes de banda ancha y mecanismos para reducir costes de implantación.

Nuevas infraestructuras públicas de servicios digitales a través de los préstamos del Mecanismo «Conectar Europa».

Con el objetivo de reducir costes, la comisión promoverá la implantación de servicios digitales de firma e identificación electrónicas.

Puesta en marcha de una gran coalición sobre las competencias digitales y el empleo.

Mediante la certificación de competencias y la creación de vínculos directos entre la enseñanza y las empresas, la Comisión pretende fomentar la cualificación profesional y así facilitar su inserción laboral.

Propuesta de una estrategia y una Directiva de la UE sobre ciberseguridad.

En el comunicado la UE, Kroes, reflexiona sobre la necesidad de la seguridad en los entornos digitales, valorando la libertad y la intimidad de los usuarios. Continúa explicando las acciones concretas que se van a realizar (Comisión Europea, 2012b):

Elaboración de una estrategia y una propuesta directiva a fin de establecer un nivel mínimo común de preparación a escala nacional para hacer frente a los ciberataques y ciberdelincuentes.

Crear una plataforma en línea para prevenir y contrarrestrar los ciberincidentes transfronterizos.

Por último, añade que de este modo se estimulará el mercado europeo de productos que incorporen la seguridad y la privacidad en el propio diseño.

Actualización del marco de la UE en materia de derechos de autor.

La Comisión, como veremos más adelante, considera imprescindible la modernización de los derechos de autor en el 'mercado único' digital. Por ello, revisará el marco legislativo de la UE sobre derechos de autor con intención de incorporar la reforma legislativa que se considere beneficiosa para este fin.

Promoción de la computación en nube mediante el poder de compra del sector público

Se pondrán en marcha acciones piloto para propulsar la computación en la Nube desde la Asociación Europea de Computación en la Nube. Uno de los objetivos, nuevamente, es conseguir que desaparezcan las percepciones negativas de los consumidores donde la seguridad de la información vuelve a ser uno de los puntos críticos de la confianza en estos servicios.

Puesta en marcha de una nueva estrategia industrial para la electrónica.

Se propondrá una estrategia industrial en beneficio de la microelectrónica y la nanoelectrónica que propicie mayor inversión con el objetivo de reforzar su cuota en el mercado mundial.

2.7 Estrategia europea 'Una mejor internet para los niños'

En los últimos años se han desarrollado una serie de políticas para mejorar las experiencias de los menores en Internet, sin embargo, usualmente eran medidas específicas centradas en los canales y plataformas digitales, sin plantearse de manera combinada en un marco coherente. Hasta el momento las políticas de la Unión Europea no han reconocido a los niños como público objetivo específico en Internet, que requiere un ecosistema propio, adaptado a sus necesidades, que les permita disfrutar de las oportunidades y beneficios de la red (European Commission, 2012).

El 2 de Mayo de 2012, la Comisión Europea presenta un plan estratégico para conseguir que los niños europeos mejoren su competencias digitales, utilizando herramientas adecuadas a sus necesidades y de este modo puedan beneficiarse de las oportunidades que presenta para ellos el mundo digital.

Neelie Kroes, Vicepresidenta de la Comisión Europea, ha declarado que los niños necesitan herramientas digitales sencillas y seguras, además de conocimientos y competencias para saber utilizarlas. Añade que esta iniciativa pretende que los menores puedan obtener servicios adecuados a su edad y contenidos de calidad, gozando de seguridad para que así puedan disfrutar de experiencias positivas en Internet (Comisión Europea, 2012a).

A través de esta iniciativa, la Comisión Europea aspira a crear un mercado de contenidos educativos e interactivos on line, mediante la cooperación entre Comisión Europea, Estados miembros, los operadores de telefonía móvil, los fabricantes de

terminales y los proveedores de servicios de redes sociales (European Commission, 2012).

Debido a la divergencia de los enfoques que se dan en cada país, los niños presentan diferentes necesidades y niveles de conocimientos, lo que hace que sea más complejo para las empresas comercializar productos a nivel internacional adaptados a los menores.

Con el fin de lidiar con las dificultades existentes la Comisión ha definido una serie de medidas que deben conducir a soluciones flexibles y rápidas, articuladas en cuatro objetivos principales (Comisión Europea, 2012a):

Fomentar la producción de contenidos creativos y educativos en línea de alta calidad, destinados a los niños. Desarrollar plataformas que ofrezcan acceso a contenidos adaptados a la edad y crear experiencias positivas dirigidas a menores.

Aumentar la sensibilización y la enseñanza de la seguridad en línea en todas las escuelas de la UE, a fin de desarrollar la alfabetización digital y mediática de los niños y la autorresponsabilización en línea.

Crear un entorno seguro para los niños en el que, tanto los padres como los menores, dispongan de las herramientas necesarias para garantizar su protección en línea (por ejemplo, mecanismos fáciles de utilizar para denunciar los contenidos y conductas nocivos en línea, parámetros de privacidad predefinidos, adaptados a la edad, que sean transparentes, o controles parentales de fácil utilización).

Luchar contra el material pornográfico infantil en línea, fomentando la investigación y la utilización de soluciones técnicas innovadoras en las investigaciones

policiales, que permita la cooperación nacional e internacional para facilitar la detección de los perpetradores.

No hay duda del interés que ha despertado en Europa desde hace unos años la seguridad en Internet. El potencial y las oportunidades que se presentan en la red no pueden ser explotadas si los usuarios no se sienten seguros y confiados al hacer uso de las tecnologías de la información y la comunicación y, más concretamente, de Internet.

Las propuestas europeas sin duda pueden cambiar el panorama de la seguridad en la red, por lo que los países miembros están acelerando el proceso de integración y creación de planes que permitan seguir las directivas europeas.

'Safer Internet' y 'Better Internet for Kids'

El programa Safer Internet, puesto en marcha en 1999, fue el primero creado con el fin de crear un Internet más seguro a través de proyectos para promover la autorregulación de la industria y la cooperación internacional. Tras la aprobación en 2012 de la "Estrategia europea para hacer de Internet un lugar mejor para los niños" que cubre todas las actividades relacionadas con la lucha contra los contenidos ilícitos, filtrado y etiquetado de contenidos, sensibilización, formación, etc., el programa *Better Internet for Kids,* es el encargado de su cumplimiento.

EU Kids Online fue financiado por el programa *Safer Internet* y posteriormente ha sido financiado por el programa *Better Internet for Kids.*

En la etapa 2009-2013 Safer Security recibió 55 millones de Euros de la Unión Europea para hacer de Internet un lugar más seguro, especialmente para los niños,

utilizados para combatir contenidos ilícitos, comportamientos nocivos en la web, etc. Además, el programa 'Internet Segura' cofinancia proyectos para (INSAFE, 2013a):

Informar o generar información dirigida a niños, padres y profesorado sobre hábitos seguros en la red.

Ofrecer a los ciudadanos lugares de denuncia de contenidos ilícitos y nocivos, especialmente si se trata de sitios web con contenidos sobre abuso infantil.

Iniciativas de empoderamiento.

Estimular la participación de los jóvenes en entornos on line que sean seguros para ellos.

Establecer una base de conocimientos sobre el uso de las tecnologías de información y la comunicación y sus riesgos, promoviendo la participación de investigadores de todos los países en éste ámbito.

El programa apoya los proyectos y eventos para ayudar a crear un entorno on line para niños y jóvenes, así como para promover la autorregulación del sector y la cooperación internacional. Realiza actividades para promover la sensibilización, la lucha contra los contenidos ilícitos, el filtrado y la clasificación de contenidos, la participación de la sociedad civil en temas de seguridad on line de los niños, así como la ampliación de una base de datos con información relacionada con el uso de las tecnologías de la información y la comunicación por parte de los menores (INSAFE, 2015c).

Los dos eventos más importantes del programa de *Better Internet for Kids*, de los que hablaremos a continuación, son el Día Mundial de Internet Segura y el Foro de Internet Segura.

Día Mundial De Internet Segura (Safer Internet Day)

Se ha creado el día mundial de 'Internet Segura', celebrado en más de 100 países (Ver Imagen abajo) bajo el lema "Derechos y Responsabilidades on line" y "Conéctate con respeto". Podemos acceder más información sobre futuros eventos en la dirección web: http://www.saferInternetday.org

Figura 25 Celebración 'Día mundial por un Internet seguro'

(Safer Internet Day, 2015)

Continent	No. of countries that celebrated SID 2015
Africa	19
Antarctica	0
Asia	27
Europe	47
North America	10
Oceania	2
South America	10
Total	115

Figura 26 Número de países que celebran el 'Día mundial por un Internet seguro'

(Safer Internet Day, 2015)

Con los años, el día de Internet segura, se ha convertido en un hito en el calendario de la seguridad on line. Nació como una iniciativa del proyecto llamado SafeBorders de la Unión Europea en 2004 y fue retomado por la 'Red Insafe'.

La celebración del 'Día mundial por una Internet segura' (DIS) se hace en todo el mundo en Febrero. En el año 2015, se celebró el día 10 de Febrero con el objetivo de promover la colaboración de todos y todas para conseguir un entorno on line sin riesgos. El lema fue 'Vamos a crear un mejor Internet juntos'. En el año 2016, la celebración fue el martes 09 de febrero bajo el lema 'Juega tu parte para crear una Internet mejor' (INSAFE, 2015a). Para este 2017, la celebración se llevó a cabo el 7 de febrero bajo el lema "Be the change: Unite for a better internet"

Los responsables de la planificación y coordinación del evento son los 'Centros de Internet Segura' de cada país, los comités del 'Día Mundial de Internet Segura' y otros colaboradores que apoyan los objetivos del evento:

Centro de Internet Segura: miembros de la red Insafe que participan en los comités DIS.

Comité del Día de Internet Segura: organización en un tercer país que ha obtenido apoyo del gobierno para las acciones del día mundial de Internet seguro. Se encarga de la gestión de fondos y recursos para ayudar a desarrollar la campaña localizada.

Apoyando al Día de Internet Segura: son los países donde el Equipo de coordinación Insafe participan en la celebración pero donde no hay comité SID oficial.

Instituciones / Industria: instituciones, industria u otros tipos de organizaciones que apoyan en la celebración del evento.

Día de Internet Segura en España 2015

El evento consistió en un congreso nacional centrado en las alianzas público-privadas y la importancia de la responsabilidad de todos nosotros. Con este objetivo, el evento se repite un año más en España con el lema 'Vamos a crear un mejor Internet juntos'.

El congreso se llevará a cabo (el resto está en pasado), en último trimestre del año, en el Ministerio de Industria, Turismo y Comercio de España, y será inaugurado por el Director general de Red.es (entidad pública empresarial encargada de promover el desarrollo de la Sociedad de la Información en España). Posteriormente, se continuará

con tres mesas de reflexión sobre la experiencia adquirida en el desarrollo de diferentes iniciativas (INSAFE, 2015b) :

Plataformas de redes sociales e ISP, en representación del sector privado y fundaciones y ONGs en representación de la sociedad civil.

El sector público: Ministerio de Educación, Cultura y Deporte, Ministerio de Salud y Servicios Sociales, los cuerpos de seguridad, la agencia de protección de datos nacional, universidades y la comunidad científica.

Grupo de trabajo público-privada: formado por más de 50 acores de todos los sectores relacionados con la protección de los menores.

Intercaladas con las mesas redondas, se llevaron a cabo dos paneles temáticos sobre el 'contenido positivo para los menores' y sobre el 'Ciberbullying: experiencias y nuevas iniciativas'. Además, a lo largo del día se presentarán los resultados de actividades de sensibilización que desarrollarán desde Pantallas Amigas.

Reflexión sobre el 'Día Mundial de Internet segura' en España

Es necesario parar un momento a reflexionar sobre el impacto que tiene la celebración del 'Día de Internet segura' en nuestra sociedad. No hay ningún estudio que nos diga la eficacia de las actividades programadas, lo que sí tenemos es la programación de actividades que se han hecho en otros países. No vamos a hablar demasiado de todo esto, analizando cada una de las actividades que se realizado en los otros países participantes, pero sí vamos a mencionar la repercusión del 'Día de Internet segura' en un país que quizás nos pueda aportar ideas para las próximas celebraciones:

La celebración del 'Día de Internet segura' en Reino Unido es coordinado por el Centro de Internet Segura del país, donde ve prioritario la participación del máximo número de organizaciones con el fin de promover el uso seguro, responsable y positivo de la tecnología on line para niños y jóvenes (UK Safer Internet Center, 2015).

En la celebración del 'Día de Internet segura' en el año 2014, consiguieron llegar al 25% de los niños del país, el 18% de los adolescentes y el 10% de los padres (UK Safer Internet Center, 2015). Quizás algunas personas puedan consideran este dato increíble o imposible de alcanzar en España, lo que sin duda podemos llegar a pensar que se antoja imposible alcanzar repercusiones similares en la celebración del día en España con las propuestas realizadas.

Es necesario que se reflexione sobre los objetivos de la celebración en el 'Día por una Internet segura' en España. Si lo que se pretende es crear impacto social es necesario programar acciones por todo el país dirigidas a menores y sensibilizarles sobre los riesgos y oportunidades de la red para los menores. La creación del 'Día mundial por una Internet segura' supone una oportunidad para los organismos encargados de la coordinación para planificar actividades que cubran el mayor número de necesidades posibles, que presentan los jóvenes para hacer un uso seguro y responsable de la red.

Foro de Internet Segura

Se trata de la principal conferencia europea sobre los problemas de la seguridad on line que se realiza desde 2004, donde los responsables políticos, investigadores, fuerzas de la ley, jóvenes, padres, maestros, ONGs, representantes de la industria,

expertos y otros actores relevantes se reúnen para discutir las últimas tendencias, riesgos y soluciones relacionadas con la seguridad on line de los jóvenes. Está financiado por el programa 'Interner Segura' como parte de la estrategia europea una conseguir una mejor Internet para los niños (INSAFE, 2015c).

En el año 2014 se celebró en Bruselas la 11º edición del foro con el tema 'Crecer digitalmente'. En el evento en el que pudieron discutir sobre las últimas tendencias, riesgos y soluciones relacionadas con la seguridad on line, participaron más de 260 actores en el campo de la seguridad on line (INSAFE, 2015c). Y en el año 2015 el foro tuvo lugar en lugar en Luxemburgo el 28 y 29 de Octubre.

INSAFE (European network of Awareness Centers)

Insafe es una red europea, integrada por 31 centros nacionales, pertenecientes a los 27 estados miembros de la Unión Europea, más Islandia, Noruega, Rusia y Serbia. Fundada en 2004, la misión de la red europea es capacitar a los niños y jóvenes a conectarse a Internet y utilizar las tecnologías de la información y la comunicación de manera segura. Cada centro nacional implementa campañas de sensibilización y educación y pone líneas de ayuda a disposición del ciudadano (Insafe, 2000).

En la Figura 27 podemos ver los países que forman parte de la red europea Insafe, disponible en su página web.

Figura 27 Países pertenecientes a la red Insafe

(INSAFE, 2015a)

Misión de Insafe:

La misión de la red de cooperación Insafe es capacitar a niños y jóvenes a utilizar las tecnologías de la información y de la comunicación de manera segura, positiva y efectiva. La red exige que la responsabilidad de proteger los derechos y necesidades de los menores es compartida por familias, educadores, gobierno, medios de comunicación e industria, además de otro agentes relevantes del entorno de los menores (Insafe, 2000).

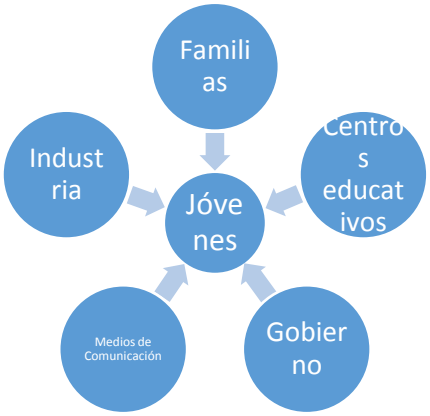


Figura 28 Convergencia de los agentes por la seguridad de los jóvenes en Internet

(INSAFE, 2013a)

¿Qué aporta Insafe? (Insafe, 2013b)

Artículos de interés para centros educativos: produce amplia información y recursos para ayudar a los centros educativos y otros formadores para crear conciencia sobre la seguridad on line.

Boletín informativo Insafe: envía a todos sus suscriptores un boletín mensual gratuito con información y temas de actualidad sobre recursos de seguridad on line directamente al correo electrónico.

Campaña 'Vuelta al colegio': Insafe dirige una campaña que proporciona herramientas, consejos y recursos para facilitar a profesorado y alumnado la vuelta a clase después de las vacaciones.

Pan-UE Plataforma Juvenil: es una plataforma digital dirigida a jóvenes de edades comprendidas entre los 14 y 18 años con el objetivo de aportar un sitio web donde los jóvenes puedan expresar sus pensamientos, ideas o conocimientos de cualquier tema relacionado con las tecnologías. En la web disponen de foros, blogs,

espacios diseñados para la publicación de vídeos o pueden dejar mensajes en el Facebook y Twitter de la plataforma.

La plataforma dispone también de juegos que estimulan el debate y la reflexión de los jóvenes en el grupo.

Recursos de la red Insafe: los centros que componen la red Insafe producen regularmente recursos on line a los que se puede acceder, además de pasar a formar parte de la base de datos de recurso que Insafe a través de su página web pone a disposición de los internautas.

Insafe/INHOPE: proporciona información sobre la red conjunta de centros de sensibilización, líneas de ayuda, líneas de denuncia y paneles de jóvenes que forman parte del programa Safer Internet de la Comisión Europea.

Centros de Internet Segura (Safer Internet Center)

Los Centros de Seguridad en Internet están integrados en el programa Safer Internet de la Comisión Europea desde su creación, pasando, posteriormente, a formar parte de la 'Estrategia Europea para una mejor Internet para los niños'.

Cada país de la red Insafe cuenta con un centro nacional responsable de las acciones que promueven la seguridad en Internet de los jóvenes, del desarrollo de las sinergias a nivel nacional y trabaja en estrecha cooperación con las entidades europeas, regionales y locales responsables (Insafe, 2000).

El listado de los Safer Internet Center en Europa es el siguiente (Protégeles y Cesicat, 2011):

- Alemania - Nummer gegen Kummer e.V. in cooperation with klicksafe

- Austria - Rat auf Draht 147
- Bélgica - Child Focus
- Bulgaria - Association Roditeli
- Chipre - Safer Internet CY
- Dinamarca - Ciberhus
- Eslovaquia - UNICEF Zodpovedne
- Eslovenia - Slovenian Association of Friends of Youth
- España - Protégeles
- Estonia - Estonian Advice Centre
- Finlandia - Mannerheimin Lastensuojeluliitto (Mannerheim League for Child Welfare)
- Francia - e-Enfance and Net Ecoute
- Grecia - Adolescent Health Unit, Second Dept. of Paediatrics – University of Athens
- Holanda - Help Wanted
- Hungría - Kek Vonal
- Islandia - The Public Health Institute/Directorate of Health
- Irlanda - Irish Society for the Prevention of Cruelty to Children (ISPCC) and SIC Ireland Parent Helpline – National Parents Council
- Italia - Save the Children
- Letonia - State Inspectorate for Protection of Children's Rights
- Lituania - RTT and Childline
- Luxemburgo - Kanner-Jugendtelefon
- Malta - Aġenzija

- Noruega - Cross Your Heart
- Polonia - Nobody's Children Foundation
- Portugal - Instituto Português do Desporto e Juventude
- Rumania - Sigur.info
- Rusia - Helpline – Safer Internet Centre, Russia
- Suiza - BRIS (Children's Rights in Society)
- Reino Unido - Professionals On line Safety Helpline. A helpline for children is provided by ChildLine in the UK.
- República Checa - Sdružení Linka Bezpečí, o.s. (Safety Line Association)

Centro Safer Security en España

El centro de seguridad en Internet está gestionado y liderado por la organización de la infancia Protégeles, en consorcio desde marzo del 2012 con el Centro de Seguridad de la Información de Cataluña CESICAT, cuyo objetivo es garantizar una sociedad de la información segura para todos. Ambas entidades disponen de sede en Madrid y Barcelona, siendo su ámbito de actuación todo el territorio español, por lo que trabajan en colaboración con entidades de referencia de cada una de las comunidades autónomas del territorio español (Protégeles y Cesicat, 2011).

El centro de seguridad en Internet de España tiene como objetivos procurar un entorno seguro para los jóvenes cuando están conectados a Internet o hacen uso de las tecnologías de la información y de la comunicación. Tiene tres tareas principalmente (Protégeles y Cesicat, 2011):

Proporcionar a los ciudadanos una vía de denuncia de contenidos ilícitos, amenazantes para los menores o relacionados con la pornografía infantil.

Creación, desarrollo y puesta en funcionamiento de 'Líneas de ayuda' a disposición de los menores que sirvan como referencia antes situaciones de riesgos experimentadas en la red.

Realizar campañas de formación y sensibilización, a través de acciones de formación en centros escolares, asociaciones de padres y madres de alumnos, cuerpos y fuerzas de seguridad y profesionales que trabajan con menores.

PROTÉGELES es la única organización española integrada en el INHOPE y en el Insafe programas dependientes de la Comisión Europea, de los que hablaremos a continuación, y en eNACSO (European NGO Alliance for Child Safety On line).

El dossier presentado por CESICAT y PROTÉGELES sobre el trabajo realizado por el 'Centro de Internet más Segura', en el periodo marzo 2012 a Junio 2014, nos informa de la demanda que ha recibido de usuarios de Internet (Protégeles y CESICAT, 2014):

Más de 149.000 comunicaciones advirtiendo de la existencia de páginas web con contenido sobre pornografía infantil y otros contenidos ilegales, transfiriéndose más de 7.000 denuncias a unidades policiales de todo el mundo.

La Línea de ayuda, recibe diariamente peticiones de ayuda a menores que sufren situaciones de acoso escolar en Internet, ya sea ciberbullying, acoso sexual, usurpaciones de identidad, etc.

Durante estos 28 meses han realizado más de 1.800 intervenciones legales y/o psicológicas

El Centro de Internet Segura ha realizado durante este periodo, además de las funciones anteriores, las siguientes actividades (Protégeles y CESICAT, 2014):

Organización de reuniones del "Comité de Expertos sobre seguridad de los menores en Internet". En él participan representantes de distintos sectores de la sociedad: representantes de las comunidades autónomas, representantes de la industria de Internet y la telefonía móvil como Google, Facebook o Telefónica, Fuerzas y Cuerpos de Seguridad del Estado, representantes del Ministerio de Sanidad, Servicios Sociales e Igualdad, sindicatos de profesores y representantes de padres y madres, etc., con el fin de aportar distintos enfoques a un mismo problema y encontrar el camino para hacer de Internet un lugar más seguro para los jóvenes.

Paneles de jóvenes: se trata de un espacio creado para los jóvenes en el que se facilita el debate sobre cuestiones relacionadas con el uso seguro de las TIC. Estos paneles en España, son coordinados por PROTÉGELES.

Congreso joven y en red: en la celebración del *Día Internacional por Internet Segura*, el centro de Seguridad en Internet celebró en Madrid el III Congreso Nacional 'Joven y en Red' bajo el lema 'Juntos podemos hacer una Internet mejor'. En él participaron niños y adolescentes, representantes de la industria en Internet, fuerzas y cuerpos de seguridad, representantes de la consejería de educación, asociaciones de padres, madres y profesores, etc., para aportar opiniones y/o conocer el momento actual por el que pasa la seguridad en Internet para los jóvenes.

Programa audiencia pública dedicada a la ciudadanía digital: a lo largo del curso académico, más de 700 alumnos y alumnas de 20 centros educativos participantes han reflexionado sobre las oportunidades de las tecnologías emergentes en la sociedad. El CESICAT que realizó una acción formativa dirigida a los coordinadores de cada centro

sobre seguridad TIC coordinó la elaboración de una guía didáctica dirigida a estudiantes y guías de orientación dirigidas a profesorado.

Durante el mes de mayo, una delegación de 250 jóvenes presentó los resultados del programa al alcalde de Barcelona reconociéndose el mérito de la misma por Naciones Unidas.

Acciones específica en Cataluña: CESICAT y el departamento d'Ensenyament, junto con la Autoridad catalana de protección de datos y Mossos d'Esquadra, han desarrollado recursos para la comunidad educativa sobre privacidad y seguridad en Internet. Además, se han desarrollado sesiones de formación dirigidas a profesionales que trabajan infancia y adolescencia.

APP PROTEGETE: Se trata de una App para Smartphones y Tablets, en cuyo desarrollo han participado niños y adolescentes, facilita la denuncia de contenidos ilícitos y la comunicación con líneas de ayuda. A día de hoy, la APP no está disponible en ninguna plataforma.

Canal Disney: durante varias semanas miles de niños y adolescentes, han podido ver el spot 'Navega Seguro' protagonizado por personajes de la serie 'Violeta".

Ciberfamilias.com: Línea de ayuda para familias disponible en www.ciberfamilias.com.

Campañas en las redes sociales más conocidas: Facebook, Twitter, instagram y Pinterest entre otras.

Formación y Sensibilización: Durante los 28 meses de funcionamiento del Centro se han realizado sesiones formativas presenciales en más de 3100 centros educativos, más de 162000 alumnos, 21000 padres y madres y 2000 profesores.

Talleres a voluntarios: se hacen talleres enfocados a voluntarios de empresas de nuevas tecnologías sobre seguridad TIC, con el fin de que las personas que participan en las sesiones realicen tareas de prevención en los centros escolares de sus hijos y/o que están en su barrio. Los empleados de algunas empresas como Microsoft, Vodafone u Orange participan en estas campañas de sensibilización en su horario laboral.

Campaña The Phonbies: desarrollada en colaboración entre el Gobierno de la Comunidad de Madrid y la fundación SmileStone. La campaña pretende fomentar la conciencia y la autorregulación entre los menores en relación al uso de los Smartphones.

Los datos cuantitativos relativos al impacto de las actividades y campañas que se han hecho público en Agosto del 2015.

INHOPE (International Association of Internet Hotlines)

Fundada en 1999, la 'Asociación internacional de líneas directas de Internet' coordina una red de 48 líneas directas en 42 países de todo el mundo, en las que se atienden las comunicaciones para denunciar contenidos ilegales on line. Fue creada con la financiación y el apoyo de la Comisión Europea a través del Programa Internet Segura (INHOPE Foundation, 1999).

Los objetivos principales de INHOPE son:

Establecer y apoyar la creación de líneas directas de denuncia de sitios web con contenidos ilícitos o dañinos.

Capacitación y asesoramiento a las nuevas líneas directas.

Fomentar la conciencia sobre la seguridad en Internet y la educación permanente.

Establecer procedimientos eficaces para la recepción y procesamiento de las denuncias.

Desde la página web de INHOPE, http://www.inhope.org/gns/home.aspx, se persigue la tolerancia cero a las imágenes con contenidos de abuso sexual en las que aparezcan niños. Además, anima a que todos formemos parte de la lucha contra estos contenidos denunciado cualquier página web que encontremos que tenga estos contenidos con el fin de eliminarla lo ante posible.

Desde la página web de INHOPE, al seleccionar el país donde te encuentras o del que deseas conocer información, te re-direcciona a la página web que gestiona los informes de denuncia de páginas web con contenidos ilícitos en dicho país. Los países que disponen de líneas de denuncia coordinadas con INHOPE, los podemos ver en la siguiente imagen:

Figura 29 líneas de denuncia coordinadas con INHOPE

(INHOPE Foundation, 1999)

Si queremos conocer la página web que gestiona las denuncias en nuestro país podemos acceder a ella a través de la página web de INHOPE.

La línea de denuncia INHOPE en España, ALIA2

La Fundación Alia2 es la entidad responsable de gestionar la iniciativa promovida por INHOPE en España cuyos objetivos son la lucha contra la pornografía infantil en Internet y el ciberacoso. En su misión, alia2, pretende salvaguardar la integridad y el desarrollo emocional e intelectual del menor cuando hace uso de las tecnologías de la información y la comunicación, mediante tres líneas de acción (Fundación Alia2, 2012):

Informar y sensibilizar a docentes y formadores, a padres y madres de familia y a los menores para que conozcan los buenos hábitos al hacer uso de las TIC.

Desarrollar herramientas informáticas para rastrear Internet con el fin de detectar, controlar y erradicar contenidos y comportamientos ilícitos.

Actualmente, además se está gestionando la plataforma de voluntariado, Ciberalia2 creada para desarrollar, mejorar y solventar las necesidades informáticas que puedan suponer un obstáculo para conseguir hacer de Internet un lugar seguro para todos.

Aunar esfuerzos: canalizan y apoyan las iniciativas de instituciones públicas o privadas, socios y voluntarios que beneficien a cumplir los objetivos de la fundación.

La Fundación Alia2 dispone de línea de ayuda para víctimas de algún tipo de abuso en la red como ciberbullying, sexting o grooming, a través de WhatsApp, correo electrónico o de la página web de Tuenti.

La fundación cuenta con un equipo de psicólogos clínicos con experiencia en atención a menores y psicólogos con experiencia en la rama jurídica y criminalista.

En la Figura 30 observamos cómo dejar una denuncia de páginas web con contenidos perjudiciales de algún modo para los menores:

Figura 30 Web Fundación Alia2

(Fundación Alia2)

Conclusiones y resultados informe INSAFE-INHOPE 2014

El informe anual Insafe – INHOPE de 2014, redes cofundadas por la Unión Europea bajo el programa Safer Internet (Insafe y Inhope, 2015) nos aporta datos relevantes en el objeto de nuestra investigación los cuales analizaremos a continuación.

Desde la creación de INHOPE hace 15 años e Insafe hace aproximadamente 10 años, ambas redes han tenido que evolucionar para hacer frente a los nuevos retos que les ha ido presentado la evolución de las tecnologías.

Si paramos brevemente a recordar, no mucho tiempo atrás vivíamos sin las redes sociales que hoy en día cuentan con millones de usuarios y que son protagonistas de gran cantidad del intercambio de la información que se produce en Internet. Por

ejemplo, Facebook cuenta con más de 1,3 millones de usuarios activos, y a través de Twitter se envían más de 500 millones de "tweets" todos los días, según datos del informe. Además, hemos podido vivir el cambio del teléfono móvil al Smartphone, la conexión a Internet a través de las televisión y próximamente veremos los relojes inteligentes que amplían sus campañas de marketing para introducirse en nuestro mercado.

Por estos motivos, las dos redes han tenido que ampliar su enfoque de la protección de los jóvenes cuando se conectan a la red. Con el apoyo de la Comisión Europea, la red conjunta Insafe-INHOPE se han reunido para hacer de Internet un lugar más seguro donde los jóvenes son el centro de todo y donde la industria es un socio importante en éste proceso de cambio. Lo único seguro en la red, es que en la próxima década seguirá evolucionando (Insafe y Inhope, 2015).

No es necesario divagar sobre la tecnología del futuro. Ya se prepara para el aterrizaje en nuestra vidas el llamado 'Internet de las cosas' con sus sensores portátiles y no portátiles conectados a la 'Big data', recolectando información. Los próximos desafíos para los expertos en seguridad en Internet ya están presentes, con viejos riesgos cambiantes y otros nuevos que aparecen al mismo ritmo que evoluciona la tecnología y que exigen nuevos recursos y enfoques, pero sobre todo un mayor esfuerzo por parte de todos los sectores de la sociedad (Insafe y Inhope, 2015).

Insafe-INHOPE continuarán luchando en su línea de especialización que va desde la innovación en la enseñanza y el aprendizaje para hacer frente a los contenidos ilícitos en la red, a las campañas de sensibilización de los riesgos y oportunidades que se presentan en Internet.

Resultados

En 2014, los Centros Safer Internet que operan como parte de articulación Insafe-INHOPE ha obtenido los siguientes resultados:

Ha trabajado con cerca de 2600 socios entre industria, organismos reguladores, investigadores, etc.

Han participado 12 jóvenes.

1380 nuevo recursos producidos.

Los recursos producidos han llegado a 22,5 millones de personas.

15000 eventos realizados que han llegado a más de 2 millones de personas.

Las líneas de ayuda recibieron 72000 informes.

Ha habido 1500000 informes a través de las líneas de denuncias de contenidos ilícitos, de las que el 57% han sido confirmados por analistas de INHOPE como materiales que contienen abuso infantil.

El 98% de los informes de abuso sexual infantil recibidos se pasaron a las agencias de las fuerzas del orden en el plazo de 1 día.

2.8 Agenda digital en Europa

La Agenda Digital Europea 2015-2020 está compuesta por dos grandes bloques que nos es necesario analizar para conocer y comprender las características que presentan en el objeto de la investigación.

Europa digital

La Agenda Digital para Europa este periodo continúa siendo uno de los siete pilares de la Estrategia para Europa 2020. La Comisión Europea, a través de su página web, publica que la Agenda Digital propone explotar el potencial de las TIC con el fin de fomentar la innovación, el crecimiento económico y el progreso de Europa, siendo el principal objetivo del programa digital desarrollar un mercado único digital para generar crecimiento sostenible, inteligente e integrador (Comisión Europea, 2015a).

Los objetivos para los próximos cinco años son:

- La realización del mercado único digital.
- Mejora de los estándares e interoperabilidad.
- El fortalecimiento de la confianza y la seguridad en línea.
- Promover el acceso a Internet rápido y ultra-rápido para todos.
- Invertir en investigación e innovación.
- Promover la e-inclusión, la alfabetización digital y la adquisición de competencias digitales.
- Explotar los beneficios que ofrecen las TIC para la sociedad.

Se puede observar que los objetivos que plantea la Comisión Europea en 2010 – 2014 y 2015 – 2020 son prácticamente idénticos. Sería necesario analizarlos individualmente para valorar las diferencias, por lo que a continuación vamos a explorar aquellos que están relacionados con el objetivo de la investigación.

El fortalecimiento de la confianza y la seguridad on line

Tras estos años en los que se ha trabajado para fortalecer y mejorar la seguridad con la que los usuarios hacen uso de Internet, tan sólo el 12% de los internautas afirman realizar transacciones y compras on line con total seguridad. El software malicioso y los fraudes on line desestabilizan la confianza de los consumidores para promover la economía digital (Comisión Europea, 2015b).

La Agenda Digital propone un conjunto de soluciones, en las que se incluye una respuesta conjunta europea a los ciberataques así como reforzar la normativa sobre la protección de datos personales.

La lista de propuestas presentadas por la Comisión Europea para la Agenda Europea con el fin de fortalecer la confianza y la seguridad on line es la siguiente (Comisión Europea, 2015c):

Acción 28: Red blindada y Política de Seguridad de información

Acción 29: Combatir los ciberataques contra los sistemas de información

Acción 30: Establecer una plataforma ciberdelincuencia Europea

Acción 31: Analizar la utilidad de crear un centro de ciberdelincuencia Europea

Acción 32: Fortalecer la lucha contra la ciberdelincuencia y los ataques cibernéticos a nivel internacional

Acción 33: Apoyar a escala comunitaria la preparación para la seguridad cibernética

Acción 34: Examinar la ampliación de las notificaciones de violaciones de seguridad.

Acción 35: Orientación sobre la aplicación de las normas sobre privacidad en las telecomunicaciones.

Acción 36: Apoyar la realización de informes de contenidos on line ilegales y las campañas de sensibilización de seguridad on line para niños.

Acción 37: Fomentar la autorregulación en el uso de servicios on line.

Acción 38: Establecer equipos de respuesta a las emergencias informáticas en los estados miembros.

Acción 39: Simulaciones de ciberataque en los estados miembros.

Acción 40: Los Estados miembros deben crear líneas de contacto para denunciar la existencia de contenidos dañinos en la red.

Acción 41: Los Estados miembros deben establecer plataformas de alerta nacionales.

Acción 123: Propuestas de directivas sobre seguridad de la información en la red.

Acción 124: Estrategia de Seguridad Cibernética de la UE

Acción 125: Ampliar la Alianza Global contra el abuso sexual infantil on line.

De todas estas acciones vamos a examinar las que directa o indirectamente están relacionadas con el objeto de la investigación.

Acción 35: Orientación sobre la aplicación de las normas en las telecomunicaciones sobre la privacidad (Comisión Europea, 2013b)**.**

Las reformas en la normativa del 25 de noviembre del 2009, traen consigo varias modificaciones sobre la directiva de privacidad y comunicaciones electrónicas y

refuerza las normas sobre el acceso a dispositivos con conexión a Internet del software como cookies, spyware o malware.

El 25 de mayo de 2011 los estados miembros de la UE pusieron en funcionamiento las nuevas normativas sobre telecomunicaciones de la Unión Europea.

En este sentido, la comisión europea ofrece orientación a los países miembros para lograr la protección correcta y efectiva de los derechos de privacidad y seguridad jurídica de la industria.

Para ello, la Comisión Europea en octubre de 2011 pidió a los países miembros que le informaran sobre el proceso de aplicación de la normativa para poder supervisar el proceso.

La comisión, por su parte, ha penalizado a los estados miembros que no han incorporado plenamente la reforma en la normativa de las telecomunicaciones.

Acción 36: Realizar informes de contenidos on line ilegales y campañas de sensibilización de seguridad on line para niños (Comisión Europea, 2013a)

Mediante esta acción se pretende proporcionar lugares de notificación y denuncia de contenidos ilegales o nocivos para los menores a disposición de los usuarios de Internet. Además pretende fomentar, mediante campañas de sensibilización, la importancia de la seguridad on line para niños a nivel nacional y mejorar la cooperación internacional para compartir las buenas prácticas existentes aumentando la eficacia de las medidas tomadas contra los riesgos procedentes de la red que afectan a los colectivos más vulnerables.

La comunicación de la Comisión Europea sobre las 'Estrategias para conseguir una mejor Internet para los niños' se adoptó en mayo del 2012.

Por otro lado, según datos de la página web de la Comisión Europea, Internet se ha convertido en uno de los principales canales de distribución de materiales (imágenes, películas, archivos de audio, etc.) con contenido erótico o pornográfico infantil. Internet Watch Foundation confirmó 1316 dominios de abuso infantil en 2009. El contenido está empeorando constando que el 44% de las imágenes recuperadas representan la violación o la tortura de un niño, siendo el 70% de las víctimas menores de 10 años.

La lucha colectiva a través de la Unión Europea es vital dado que se trata de un problema global. El abuso se da en un lugar y se sube a la red desde un solo lugar, a priori, pero la descarga puede darse en cualquier parte del mundo. Esto hace que sea mucho más difícil detectar y localizar a los malhechores, por lo que se necesita la cooperación internacional para aumentar las probabilidades de éxito.

Estos efectos son relativamente nuevos, por lo que es importante que se actúe rápidamente para evitar que se propague y se extiendan estas acciones.

Dentro de esta acción, la Comunidad Europea en 2012 desarrolló las estrategias para conseguir una *Mejor Internet para los niños* (Strategy for a better Internet for children), vistas anteriormente, que podremos ver detenidamente en el apartado titulado '*Estrategias para conseguir una mejor Internet para los niños'*.

Cooperación Internacional:

Acuerdo Unión Europea / Estados Unidos para hacer de Internet un lugar más seguro y mejor para los niños.

Acuerdo de participación de Rusia en las redes INSAFE y INHOPE

Actividades concretas de la comisión en 2014 y en adelante

Recopilar y difundir información sobre las campañas de sensibilización y sobre las líneas de ayuda, así como de los resultados obtenidos por los centros de Internet Segura (Safer Internet) de Europa.

Apoyar la labor de los centros de Internet segura.

Dar seguimiento al programa Internet Segura en el periodo 2014 – 2020

Organizar el día de Internet Segura en 2014, y en los años venideros (11 de febrero de 2014).

Continuar con las labores de 'notificación y retirada' de imágenes de abuso infantil y fortalecer la cooperación con los investigadores de abusos sexuales infantiles on line entre los estados miembros, a través de la 'Alianza Mundial contra el abuso infantil on line'.

Continuar apoyando la cooperación internacional.

Acción 125: Ampliar la alianza global contra el abuso sexual infantil on line

Ésta acción se puso en marcha en diciembre de 2012, en estrecha colaboración entre los estados miembros de la Unión Europea y Estados Unidos, con el fin ayudar a las víctimas de este tipo de actos y encontrar a todos los responsables de las redes de pornografía infantil en línea. La colaboración se hizo necesaria debido a que se trata de un delito que no conoce fronteras, operando, cada vez más, los delincuentes de pornografía infantil a través de grupos on line internacionales utilizando protocolos de seguridad y tecnología sofisticados para frustrar los esfuerzos de las fuerzas del orden para encontrarlos (European Commission, 2014).

Uno de los objetivos de la alianza global contra el abuso sexual infantil on line es establecer una red de cooperación entre las unidades policiales especializadas de cada país participante para facilitar las investigación transfronterizas y aumentar la rapidez de actuación de las fuerzas de seguridad. Además, los países participantes se comprometen a buscar y neutralizar materiales de pornografía infantil on line.

Acción 40: Los Estados miembros deben crear líneas de contacto para denunciar la existencia de contenidos dañinos en la red

Esta acción está dirigida a la aplicación de medidas para denunciar contenidos ilegales on line, organizar campañas de sensibilización sobre la seguridad on line para los niños y ofrecer formación sobre seguridad en la red y alfabetización digital en los centros educativos. Además, los estados miembros también deben fomentar que los proveedores de servicios on line implementen medidas de seguridad en la red para menores desde 2013 (European Commission, 2013).

Además, la Comisión Europea ha promovido la creación de una evaluación comparativa de las políticas de Internet más seguras, incluyendo un análisis de los recursos utilizados para llevar a cabo estas actividades y valorar su propagación a otros países de la Unión Europea.

Podemos observar que las acciones no son independientes, sino que se interrelacionan entre sí. La comisión apoya el desarrollo de líneas de denuncia de contenidos ilegales y crea una estrategia para crear una mejor Internet para los niños dotándoles de habilidades digitales y herramientas que les permitan aprovechar las

oportunidades que les presenta Internet (acción 36) y fomenta la autorregulación de los proveedores de servicios europeos (acción 37).

Por otro lado, mientras que estas acciones estén coordinadas por la Unión Europea han de ser implementadas a nivel nacional, por lo que los Estados miembros han de proporcionar el apoyo financiero y político necesario a los centro de Internet Segura para que puedan alcanzar sus objetivos. Por último, es de vital importancia que los países miembros desarrollen estrategias adecuadas para enseñar seguridad on line en los centros educativos.

SOCIEDAD DIGITAL

Ciberseguridad

No vamos a desviar demasiado nuestra atención a este campo, pero sí es necesario que hablemos brevemente de los programas y acciones que la Comisión Europea ha emprendido para aumentar la seguridad de los usuarios de Internet.

Es inevitable que los riesgos que afectan a los usuarios de Internet afecten también a los menores. En ocasiones afectarán en menor medida, o no afectarán a los jóvenes. Esto dependerá de la utilidad de las TIC a la que nos refiramos.

Sin ánimo de profundizar en ello, por ejemplo, las personas que hacen compras por Internet, dependiendo del sistema de pago y verificación que utilicen, se pueden enfrentar a que otras personas malintencionadas accedan a sus datos bancarios o datos de su tarjeta de crédito, o simplemente que sean engañados y no reciban el producto o que el producto que llega a sus domicilios no corresponda con el que escogieron a través de la web. En este caso, las personas que no realizan compras por Internet no se

enfrentan a estos peligros pero, en cambio, si pueden víctimas de software malintencionado con la intención de robarles datos personales.

Hay, por tanto, riesgos que afectan a las personas que realizan determinadas actividades en Internet, que visitan páginas web concretas o que se dirigen a personas que dispongan de determinados programas informáticos como ocurre con los virus que afectan a unos u otros navegadores web.

Por todo ello, estas iniciativas y programas desarrollados por la Comisión Europea afectan, directa o indirectamente, a los jóvenes cuando están conectados a la red por lo que es necesario que hablemos, aunque sea brevemente de ellos:

Anteriormente, en el punto llamado el *Fortalecimiento de la confianza y la seguridad on line* hemos mencionado 17 acciones que están siendo coordinadas y gestionadas por la Comisión Europea. De las 17 acciones están enfocadas a mejorar la ciberseguridad en Europa. Éstas incluyen el establecimiento de una red de CERT (Equipos de Respuesta a emergencias informáticas) a nivel nacional que cubra toda Europa, simulaciones de respuesta a ciberincidentes y el apoyo a toda la UE para la preparación de la ciberseguridad (European Commission, 2015b). Añade, fortalecer la seguridad y resistencia de las infraestructuras TIC estimulando y apoyando el desarrollo de las capacidades de preparación, seguridad y resistencia tanto a nivel nacional como a nivel de la UE.

Además, la estrategia de ciberseguridad de la Unión Europea y las propuesta de la Comisión para crear una directiva sobre redes y seguridad de la información

presentan medidas legales para hacer más seguro en entorno on line en la Unión Europea (European Commission, 2015b).

La privacidad on line

La privacidad de la información de cualquier persona cuando está conectado a la red es uno de los 'quebraderos de cabeza', tema de reflexión y debate que más controversia han creado en los últimos años.

Al navegar por Internet proporcionamos información vital al proveedor de servicios de Internet, como actividades o páginas web que visitamos, dirección, teléfono, datos de tarjetas de crédito, etc. Toda esta información, que pasa de nuestro ordenado al dispositivo que nos conecta a la red, podría caer en manos de personas que puedan actuar en contra de nuestros intereses. Por ello, la Unión Europea ha establecido normas para garantizar que los datos personales gozan de un alto nivel de protección en toda la Unión Europea.

Sin ahondar en una revisión de las leyes, dado que se hará en un punto aparte más ampliamente, vamos a mencionar brevemente las directivas y leyes que se han creado desde la Unión Europea en cuanto a la privacidad on line.

Desde 1995 la Unión Europea comenzó a crear directivas para garantizar la seguridad de los datos personales. En 2012, la Comisión Europea propuso una importante reforma del marco jurídico de la Unión Europea sobre la protección de datos personales que fortalecen los derechos individuales.

El 12 de Julio del 2002 se crea una Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de datos personales y para garantizar el derecho a la

intimidad en el sector de las comunicaciones electrónicas. En 2009 se actualizó para proporcionar reglas más claras sobre los derechos sobre la privacidad del internauta, como el tratamiento que se hace con la información conocida como 'cookies' y sobre las violaciones de datos personales. En 2013 la Comisión pone en marcha nuevas reglas específicas para garantizar que las violaciones de datos personales en el sector de las telecomunicaciones (European Commission, 2015a).

Inversión de la Unión Europea

La investigación en este ámbito se considera fundamental para prevenir la ciberdelincuencia, mejorar la privacidad on line y garantizar la protección de los derechos fundamentales. Se deben analizar diferentes perspectivas tecnológicas, económicas, legales y sociales para promover la innovación y el crecimiento económico en la Unión Europea, garantizando la protección y los derechos fundamentales de las personas (European Commission, 2014).

A todas las investigaciones dentro de éste ámbito es necesario darle una dimensión económica y social para garantizar la seguridad y privacidad en el ecosistema digital para que así sea sostenible en el mercado interior.

Las prioridades de investigación abordan los siguientes temas (European Commission, 2014):

- Confianza en la red y en las infraestructuras de servicios.
- Gestión de la privacidad y desarrollo de software seguro.
- Informática de confianza
- Criptología, biométrica Avanzada, etc.

La Comisión Europea apoya la investigación y la innovación en el campo de la ciberseguridad, la confianza en las TIC y la privacidad (European Commission, 2014):

Hasta finales de 2013:

Financió investigación en el marco de la Investigación y Desarrollo Tecnológico.

Se realizó el 'Programa de apoyo a la política sobre competitividad e Innovación TIC' (CIP ICT-PSP) cuyo objetivo es el de estimular la confianza y seguridad en las TIC.

Desde 2014 en adelante:

Horizont 2020 es el marco general de Investigación, que proporciona desarrollo e innovación en ciberseguridad y privacidad on line.

Líneas de ayuda y Líneas de denuncia

Desde 2001 a 2013 se han contabilizado más de 300.000 informes recibidos sobre pornografía infantil y otros contenidos ilegales, de los cuales se han cursado 22.000 denuncias a unidades policiales de todo el mundo. En los últimos 5 años, se han realizado más de 4.000 intervenciones psicológicas de menores afectados por los riesgos procedentes de la red, gestionados a través de las líneas de ayuda. Durante el trabajo realizado como entidad responsable del Centro de Intervención Ante el Abuso Sexual Infantil –CIASI-, que depende de la Comunidad de Madrid, se han atendido una media de 350 casos cada año, prestando atención jurídica y psicológica a los niños y sus familias.

Se estima que la línea de denuncia de PROTÉGELES recibe en la actualidad una media de 3.500 a 5.000 denuncias mensuales sobre contenidos que engloban desde el odio racial, la bulimia y anorexia, la pornografía infantil, u otros contenidos que puedan suponer una amenaza para niños o adolescentes.

Campañas de prevención y formación

La entidad realiza talleres de prevención y formación sobre seguridad en el uso de Internet y las TIC, en los que han participado más de 180.000 alumnos y alumnas, repartidos en más de 2.500 centros educativos del territorio español.

La organización funciona bajo las exigencias y controles que impone INHOPE y la Comisión Europea. Además, cuenta con el respaldo y reconocimiento de distintos Ministerios, del Defensor del Menor, de la Policía y de la Guardia Civil entre otras instituciones.

3. Iniciativas españolas para la creación de una Internet segura para los menores

En un momento en el que la sociedad de la información no pertenece, ni en concepto ni en forma, al entorno habitual de ciudadano medio español el desarrollo de las tecnologías y de Internet comienza a sentirse en el mundo entero. En 1999 en EEUU más de 110 millones de personas tienen acceso a Internet, lo que supone un 41% de la población. En otros países, como Reino Unido, el 23% de los habitantes dispone de conexión a Internet, sin embargo, en España tan solo el 7,3% de personas se conectan en España (Comisión Interministerial de la Sociedad de la Información y de las Nuevas Tecnologías, 2000).

Ante esta situación de vulnerabilidad, los diferentes gobiernos que han pasado por el Estado español han desarrollado y apoyado diferentes iniciativas de desarrollo tecnológico, algunas de las cuales vamos a examinar a continuación.

3.1 INFOXXI

En el año 2000, el Gobierno de España aprobó la primera estrategia para el desarrollo de la Sociedad de la Información, que se concretó con el plan de acción 2001 – 2003 'INFO XXI: la Sociedad de la Información para todos', con el objetivo de dar respuesta a los objetivos establecidos en la Estrategia e-Europe y en la Estrategia de Lisboa.

El objetivo de la propuesta es "implantar la Sociedad de la información en España para que todos sus ciudadanos y empresas puedan participar en su construcción

y puedan aprovechar las oportunidades que ésta ofrece para aumentar la cohesión social, mejorar la calidad de vida y de trabajo y acelerar el crecimiento económico" (Comisión Interministerial de la Sociedad de la Información y de las Nuevas Tecnologías, 2000). El impulso al desarrollo de la Sociedad de la Información, en el que se enmarca el Plan de Acción INFO XXI, se articula en cuatro grandes líneas (Tomé Muguruza, 2001):

El acceso y la información de todos los ciudadanos a las TIC. Desde los más jóvenes, aún inmersos en la fase educativa, hasta los colectivos potencialmente más expuestos al riesgo de 'automarginación'.

La incorporación de las TIC en las empresas, para la mejora de su productividad y como herramientas básicas de competitividad.

La potenciación de la Administración electrónica, a todos los niveles: administración general del Estado, administraciones autonómicas y administraciones locales.

El fomento de los contenidos digitales: España en la red.

Podemos observar que las cuatro líneas de desarrollo, facilitadas por el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información Baudilio Tomé Muguruza, no mencionan explícitamente preocupación por los riesgos de seguridad que puedan surgir en el desarrollo de las tecnologías. El plan está centrado en la importancia de facilitar el acceso a la sociedad de la información para empresas y particulares, la administración electrónica y los contenidos digitales (Chamorro, 2001). Sin embargo, sí menciona que para alcanzar los objetivos de INFO XXI se necesita un marco regulador que aporte seguridad y confianza.

En el documento original, verificando lo dicho por Chamorro (2001), se considera esencial generar confianza entre la población y aumentar la seguridad de los sistemas de cifrado para generar confianza de empresas y consumidores en el comercio electrónico.

Además, se desarrolla el proyecto CERES que permite el cifrado y firma digital de documentos, garantizando la confidencialidad, integridad y autenticidad de los mensajes que se envían desde y hacia la administración. Se vislumbra que el proyecto en el futuro se proponga aumentar la confianza de la sociedad, pero, de momento, está centrado en la administración.

A pesar del valor que ha adquirido la seguridad en Internet hasta el momento, los programas que se desarrollan no se enfocan en crear acciones que nos permitan hacer frente a los riesgos que hoy por hoy conocemos y, en ningún caso, a los que pueden afectar a los menores.

Por último, se menciona brevemente la ampliación de las relaciones sociales en la sociedad de la información, más centrada en articular la comunicación instituciones-ciudadano, que en la comunicación entre ciudadanos, dejando 'una puerta entreabierta' a los peligros posibles de la utilización masiva de las TIC.

3.2 España.es

El programa España.es pretende implantar la Sociedad de la información y la promoción de la innovación tecnológica, siguiendo directrices estratégicas desarrollas por la 'Comisión Especial de Estudio del Desarrollo de la Sociedad de la Información', conocida por Comisión Soto (Ministerio de ciencia y tecnología, 2003).

Consta de seis líneas maestras que se dividen en 10 medidas que podemos apreciar en el cuadro de abajo:

Tres verticales: Administración Electrónica, Educación y PYMEs.

Tres horizontales: Accesibilidad y formación, contenidos digitales y comunicación.

MEDIDA		DESCRIPCIÓN	RESPONSABLE
I. administración.es			
1	Impulsar decididamente la Administración Electrónica	Ejecutar las 19 medidas del Plan de Choque	MAP liderará a través CSIAE y C. sectorial. MCyT (con Red.es) ofrecerá apoyo técnico
II. educación.es: Del "aula de informática" a la "informática en el aula", integrando las nuevas tecnologías como herramienta habitual en el proceso de enseñanza/aprendizaje. Actuación que se extenderá al periodo 2004-2007			
2	Internet en la Escuela – Infraestructuras	Acceso inalámbrico y proyector en las 53.000 aulas de los 6000 centros públicos de secundaria y FP G. Superior y G. Medio	El MECD y el MCyT (a través de Red.es) en corresponsabilidad con las CC.AA
3	Internet en la Escuela - Docentes	Ordenador portátil a los 140.000 docentes de secundaria y FP y cursos de formación	
4	Internet en la Escuela – Herramientas y Contenidos Educativos	Portal educación.es con contenidos, creación de Comunidades virtuales y servicios para la comunidad educativa (profesores, alumnos y padres).	
III. pyme.es			
5	Incorporación de las PYMEs a la Sociedad de la Información	De una manera coordinada e integrada, desarrollar e implantar soluciones y servicios, y formar a las PYMEs menos integradas en la S.I.	MinEco y MCyT en colaboración con asociaciones sectoriales, grandes empresas y CC.AA.
IV. navega.es: Accesibilidad de todos los ciudadanos a la Sociedad de la Información, acercando la S.I. a todos aquellos colectivos menos integrados a través de dotación de infraestructuras y plan de formación			
6	Telecentros (Internet Rural y en Bibliotecas – Fase II)	Instalar 2000 nuevos centros de acceso público a Internet en áreas rurales, con Banda Ancha	MCyT (a través de Red.es) y MAPA, conjuntamente con CC.AA. y CC.LL:
7	Formación e Integración Digital	Creación de la Fundación Navega.es para gestionar los programas de formación	Fundación formada por MTAS, MinEco, MECD y MCyT, sector privado y Cajas de Ahorro, en coordinación con CC.AA. y CC.LL.
V. contenidos.es: Crear contenidos Digitales de calidad, ofreciendo a la sociedad contenidos de titularidad pública y promover un uso más seguro de Internet			
8	Patrimonio.es	Digitalización, difusión y explotación de elementos del Patrimonio Histórico-artístico	Red.es en corresp. con org. culturales, CC.AA. y sector privado
9	Seguridad.es	Fomentar la seguridad y la eConfianza	Red.es
VI. comunicación.es: Comunicar a toda la sociedad las ventajas de la S.I., creando una marca para todas las actuaciones, y con una campaña "paraguas" y compañas específicas. Responsable el MCyT			

Figura 31 Líneas maestras España.es

(Ministerio de ciencia y tecnología, 2003)

Como podemos apreciar para satisfacer el V objetivo que propone ‘Crear contenidos Digitales de calidad, ofreciendo a la sociedad contenidos de titularidad pública y promover un uso más seguro de Internet’ el programa plantea ‘Fomentar la seguridad y la eConfianza.

Seguridad.es

La Administración General del Estado actuó en las dos grandes áreas de contenidos que se incluían en esta medida: seguridad y control de acceso a menores.

La seguridad estaba focalizada en un punto de vista técnico, como la afección de los virus a los sistemas informáticos o las vulnerabilidades de los sistemas. Por ello, el CERT evoluciona adquiriendo nuevas y mejoradas funcionalidades de diseminación de información, gestión de incidencias, directrices sobre seguridad e I+D. Ésta labor es encomendada a Red.es, en coordinación con centros universitarios nacionales y extranjeros competentes en seguridad.

Contenidos para menores

En un primer acercamiento a cubrir las necesidades de los menores, se propone crear contenidos de todo tipo adaptados para los menores y el control de acceso a contenidos inapropiados de Internet, centrando su atención en los contenidos de tipo pornográfico, violento o racista.

En el periodo durante el cual se desarrolló el programa se buscó garantizar la Navegación Segura, en las siguientes líneas (Ministerio de ciencia y tecnología, 2003):

- Persecución de contenidos ilegales como la pornografía infantil.
- Promover la clasificación de contenidos por la propia industria.
- Facilitar filtros de contenidos que utilicen la clasificación de contenidos creada.
- Formación y difusión de información sobre hábitos seguros cuando los niños se conectan a Internet, dirigidos a familias y profesorado.

- Recomendación de contenidos, especialmente para niños, a través de www.chaval.es

Por otro lado, el Plan de Acción eEurope 2005, aprobado por la Comisión Europea en 2002, centrado especialmente en la conectividad a Internet en Europa, propone crear un grupo de ciberseguridad, proponiendo la construcción de una cultura de seguridad en el diseño e implementación de productos de información y comunicaciones.

3.3 Plan Avanza

Enmarcado en la Estrategia de Lisboa del año 2000, el Plan Avanza fue aprobado por el Consejo de Ministros el 4 de Noviembre de 2005 y se integró en el eje estratégico de impulso al I+D+i que puso en marcha el Gobierno a través del Programa Ingenio 2010.

El Plan Avanza que cubriría el periodo 2006 – 2010 se orientó a conseguir la adecuada utilización de las TIC para "contribuir al éxito de un modelo de crecimiento económico basado en el incremento de la competitividad y la productividad, la promoción de la igualdad social y regional, y la mejora del bienestar y la calidad de vida de los ciudadanos" (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2005)

La sociedad de la información en aquella etapa en España se podía valorar de escaso crecimiento o incluso estancada. Los indicadores utilizados en los estudios analizados referentes al uso de las TIC mostraban que España se quedaba rezagada en lo que podríamos llamar la 'carrera digital'. Algunos de indicadores analizados fueron

(Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2005):

El 62% de las microempresas no veían utilidad a las nuevas tecnologías.

El 45,1% de los hogares españoles presentaba una actitud de rechazo hacia las nuevas tecnologías.

El número de usuarios de Internet estaba estancado en el 33%.

La percepción de utilidad de la red reflejó una caída sostenida del 9,2%.

Estos datos sacados del observatorio Red.es en aquellos años mostraron una preocupante realidad que colocaba a España en situación de vulnerabilidad en el desarrollo tecnológico frente al crecimiento que experimentaron otros países.

Esta situación provocó la reacción del Gobierno de España con la creación del Plan Avanza, el cual se estructuraba en torno a cinco grandes áreas de actuación (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2005):

Hogar e inclusión de ciudadanos. Se pretende desarrollar medidas que permitan que las TIC lleguen a los hogares españoles y potenciar la inclusión de los ciudadanos.

Competitividad e Innovación. Dirigida a las PYMEs, busca impulsar el desarrollo TIC en España mediante la adopción de soluciones tecnológicas.

Educación en la Era Digital. Incorporación de las TIC en el proceso educativo y en la formación en general.

Servicios Públicos Digitales. Digitalizar servicios de las administraciones públicas que faciliten trámites y gestiones a empresas y ciudadanos.

El contexto digital. Potenciar que el despliegue de infraestructuras de banda ancha llegue a todo el país y genere confianza, proporcionando mecanismos de seguridad avanzados y promoviendo la creación de nuevos contenidos digitales.

De las áreas creadas, veamos con mayor profundidad las que afectan directamente a los menores.

Educación en la era digital

Vamos a examinar brevemente éste área de actuación por su gran implicación que tiene en la seguridad con la que los jóvenes hacen uso de las tecnologías de las TIC y más concretamente de Internet.

En la Figura 32 se presenta los objetivos planteados para satisfacer las necesidades que se presentan en el área de actuación:

Objetivos Educación en la Era Digital				
Objetivo	**Indicador**	**Valor 2004**	**Valor EU2004 UE15**	**Meta 2010**
Reforzar el equipamiento existente en los centros	E1. Número de alumnos y alumnas por ordenador conectado a Internet en banda ancha	--	--	2 (según modelo educativo de cada CCAA)
	Centros educativos universitarios y no universitarios con acceso a banda ancha y a equipamiento TIC en los espacios docentes	--	--	100%
Aumentar la confianza en el uso de las TIC	E2. Porcentaje de particulares que ha utilizado Internet para fines de aprendizaje y docencia. Actividades educativas oficiales.	6,5%	11,5%	30%
	Tiempo de uso de equipamiento TIC en horario lectivo.			50%
Formar en el uso de las TIC	Docentes universitarios y no universitarios con formación tecnológica y metodológica en el uso de las TIC			75%
	Familias con acceso a formación y asesoramiento en el uso de las TIC			75 %
Incrementar la oferta de contenidos y aplicaciones TIC para educación	Porcentaje del currículo oficial de la enseñanza no universitaria soportado con contenidos educativos digitales de calidad			100%
	Porcentaje de asignaturas de titulaciones universitarias que se pueden cursar on-line			25%
Accesibilidad (Reducir la brecha digital)	Porcentaje de alumnado con necesidades educativas especiales con acceso a equipamiento TIC adaptado	--	--	70%

Figura 32 Objetivos Educación en la Era Digital

(Secretaría de Estado de las Telecomunicaciones y para la sociedad de la información, 2005b)

Se puede apreciar que los objetivos están centrados en dotar de equipamiento e infraestructuras TIC, realizar acciones formativas, crear contenidos digitales y hacer frente a la brecha Digital. No podemos saber con exactitud si dentro de los planes de formación a profesorado y familias están incluidos contenidos formativos sobre el uso seguro de los dispositivos, plataformas y contenidos que se le están facilitando, y de las habilidades digitales que se les aportará a los jóvenes. Lo que sin duda, entendemos es

que si se satisfacen las necesidades expuestas en los centros educativos y procesos formativos, los centros se sitúan en una posición privilegiada para proporcionar a familias y jóvenes conocimientos sobre el uso seguro y responsable de las tecnologías de la información y la comunicación. Esta situación de privilegio del centro también puede ser vista como una responsabilidad para quien realiza acciones formativas en dispositivos o herramientas digitales, formar en los hábitos seguros en el uso de las TIC.

El nuevo contexto digital

La otra gran área de actuación relacionada con el propósito de la investigación es lo que se ha denominado "El nuevo contexto digital".

En el área se analiza desde los "bajos índices de concienciación", respecto a la seguridad de la información de ciudadano y empresas, y la ausencia de organismos responsables de la gestión de la seguridad de la información en número y dimensión requerida (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2005).

Para hacer frente a las necesidades detectadas han creado un objetivo dentro del área: "El nuevo contexto digital" llamado e-Confianza, en el que se pretende:

Aumentar el grado de concienciación, formación y sensibilización de los ciudadanos, empresas y administraciones públicas en cuanto a la seguridad en las TIC.

Impulsar la identidad digital.

Incorporar la seguridad de la información en las organizaciones como factor crítico para aumentar su competitividad.

Desarrollar una infraestructura eficaz que garantice la seguridad de la información.

Para poder cumplir los objetivos planteados se incorporan las siguientes medidas:

Objetivos el Nuevo Contexto Digital – e-Confianza					
Indicador		**Valor España 2004**	**Valor UE15 2004**	**Objetivo**	**Meta 2010**
Empresas con acceso a Internet con problemas de seguridad (I.2)		29%	27%	Disminuir el número de **empresas** con acceso a Internet que tienen problemas de seguridad	10%
Particulares que han tomado precauciones de seguridad (I.3)	Instalación de un programa antivirus	23%	No disponible	Aumentar el número de **particulares** que toman precauciones de seguridad	60%
Empresas que han tomado precauciones de seguridad (I.4)		87%	89%	Aumentar el número de **empresas** que toman precauciones de seguridad	95%
Difusión del DNI-e		No aplica	Finlandia, Italia y Holanda, entre otros países, están realizando esfuerzos para la creación de una identidad digital	Promover el uso de la Identidad Digital	100% de la ciudadanía con DNI-e

Figura 33 Objetivos el Nuevo Contexto Digital e-Confianza

(Secretaría de Estado de las Telecomunicaciones y para la sociedad de la información, 2005b)

Objetivos Educación en la Era Digital				
Objetivo	**Indicador**	**Valor 2004**	**Valor EU2004 UE15**	**Meta 2010**
Reforzar el equipamiento existente en los centros	E1. Número de alumnos y alumnas por ordenador conectado a Internet en banda ancha	--	--	2 (según modelo educativo de cada CCAA)
	Centros educativos universitarios y no universitarios con acceso a banda ancha y a equipamiento TIC en los espacios docentes	--	--	100%
Aumentar la confianza en el uso de las TIC	E2. Porcentaje de particulares que ha utilizado Internet para fines de aprendizaje y docencia. Actividades educativas oficiales.	6,5%	11,5%	30%
	Tiempo de uso de equipamiento TIC en horario lectivo.			50%
Formar en el uso de las TIC	Docentes universitarios y no universitarios con formación tecnológica y metodológica en el uso de las TIC			75%
	Familias con acceso a formación y asesoramiento en el uso de las TIC			75 %
Incrementar la oferta de contenidos y aplicaciones TIC para educación	Porcentaje del currículo oficial de la enseñanza no universitaria soportado con contenidos educativos digitales de calidad			100%
	Porcentaje de asignaturas de titulaciones universitarias que se pueden cursar on-line			25%
Accesibilidad (Reducir la brecha digital)	Porcentaje de alumnado con necesidades educativas especiales con acceso a equipamiento TIC adaptado	--	--	70%

Figura 34 Objetivos Educación en la Era Digital

(Secretaría de Estado de las Telecomunicaciones y para la sociedad de la información, 2005b)

En la Figura 34 podemos observar que las medidas planteadas para mejorar la seguridad con las que las personas hacen uso de las TIC. Propone "Aumentar el número de particulares que toman precauciones en Internet", tomando como indicadores la instalación de un programa antivirus y, podemos deducir, aquellos que han tomado alguna otra medida de precaución.

Al mismo tiempo del Plan Avanza I, pero en otro documento, fueron publicados los anexos donde se especifican las medidas por áreas de actuación. En él podremos analizar las medidas incluidas en el área de e-confianza.

Plan Avanza Anexo I. Plan de trabajo 2006. Medidas por áreas de actuación.

e-confianza

En el Anexo I del Plan Avanza publicado a finales del 2005 en el que se plantean las Medidas por áreas de actuación en 2006 hay un cambio muy importante en las políticas planteadas por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la información para hacer frente a los riesgos derivados de las TIC que afectan a la sociedad española. A continuación, vamos a exponer las medidas planteadas con éste fin.

Difusión, Comunicación y Divulgación

El objetivo planteado pretende, además de elevar el grado de concienciación materia de seguridad como exponía el primer informe del Plan Avanza, informar a los usuarios de los riesgos derivados de las TIC que atentan contra su privacidad, dignidad o cualquier otro derecho, prestando especial atención a los menores y a otros grupos sociales vulnerables.

Para satisfacer el objetivo se realizarán campañas de sensibilización y "se crearán plataformas para la protección del menor en Internet, protección contra spam y contra los fraudes de Internet" (Secretaría de Estado de las Telecomunicaciones y para la sociedad de la información, 2005b).

Desarrollo de una red de centros de seguridad

Mediante la creación de centros de seguridad y el establecimiento de procedimientos y protocolos que permitan coordinar sus funciones, se pretende dar respuesta a los incidentes de seguridad.

En la red de centros se creará una unidad de lucha contra la violación de la privacidad que se encargue de luchar contra el spam, el phising y otros fraudes.

Extensión de las mejores prácticas asociadas a la seguridad y autorregulación

Parte del objetivo de ésta medida es el desarrollo de esquemas de autorregulación centrados especialmente en la lucha contra el spam y para la protección de los menores.

Actuaciones para la seguridad de la información

Se propone crear foros de discusión y divulgar mejores prácticas, más seguras, cuando se utilizan las TIC y realizar estudios que evalúen los avances conseguidos en la mejora de los hábitos de seguridad en el uso de las tecnologías. (Secretaría de Estado de las Telecomunicaciones y para la sociedad de la información, 2005b)

Contenidos Digitales

En el área de contenidos digitales, se propone facilitar la creación de nuevos productos y servicios basados en la información y datos generados por los ciudadanos que permitan las entidades privadas crear productos beneficiosos para ciudadanos y empresas, mediante la creación de un plan que permita reutilizar la información respetando las medidas impuesta por la Unión Europea.

La creación de contenidos digitales adaptados a las necesidades de los usuarios es vital para maximizar las oportunidades que se presentan a través de Internet y, al mismo tiempo, el uso de los contenidos adaptados y seguros es beneficioso en términos de seguridad en Internet para los jóvenes.

Plan Avanza Anexo II. Medidas por áreas de actuación 2007-2010

Del mismo modo que en el anexo I vamos a examinar brevemente las áreas de actuación de e-confianza y contenidos digitales.

e-confianza

En el año 2007 fue necesario prever la replanificación del plan avanza tras un año desarrollando las medidas establecidas previamente.

En lo que a seguridad en Internet se refiere, el área de e-confianza en la etapa 2007 – 2010 presentó las siguientes medidas (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2005a):

Promoción e Impulso al Desarrollo e Innovación de Tecnologías de Seguridad

La medida impulsa la innovación y el desarrollo de productos de seguridad en el sector TIC, utilizando los datos que se han obtenido del estudio de las necesidades de los usuarios. Para cumplir la medida, primeramente, se identificarán las necesidades y requisitos de los usuarios y, de este modo, las empresas desarrolladas de software y hardware podrán acceder a los resultados obtenidos para desarrollar sus productos atendiendo a las necesidades de los usuarios.

Promoción de la Certificación de la Seguridad, Productos, Servicios y Procesos

Potenciando y promocionando la evaluación y certificación de la seguridad de las TIC, tanto de productos como servicios, lo usuarios podrán conocer cuáles cumplen estas especificaciones y aumentar de este modo su confianza.

Contenidos Digitales

Se busca impulsar la creación de contenidos digitales a través de la creación de un observatorio y un foro que permita analizar en profundidad la situación actual de la industria de contenidos digitales para posibilitar su desarrollo.

La creación de contenidos digitales de calidad y seguros influye directamente sobre la confianza, seguridad y las oportunidades que pueden disfrutar los usuarios de Internet. Mediante éste objetivo se pretende motivar y facilitar a la industria su incorporación en un mercado aún en desarrollo de contenidos digitales.

Balances de actuaciones de fomento de la Sociedad de la Información de 2008

La 'Secretaría de Estado de telecomunicaciones para la sociedad de la información,' a petición del Gobierno, en Marzo del 2008 hace público un documento en el que sintetiza las medidas y actuaciones para el fomento de las telecomunicaciones, el desarrollo de la Sociedad de la Información y la reforma del Sector Audiovisual, que nos permite explorar los resultados obtenidos por el Plan Avanza. Además, se exponen las medidas tomadas para cumplir los propósitos establecidos.

Antes de entrar en valoraciones, el documento reduce todas las medidas y objetivos tomados por el plan Avanza a uno sólo objetivo prioritario: Conseguir que el volumen de actividad económica relacionada con las TIC llegue al 7% del PIB en 2010. Las medidas propuestas se enfocan encaminadas a "conseguir la adecuada utilización de

las TIC para contribuir al éxito de un modelo de crecimiento económico basado en el incremento de la competitividad y la productividad, la promoción de la igualdad social y regional y la mejora del bienestar de la calidad de vida de los ciudadanos" (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2008)

Se debe de tener en cuenta que se produce un gran incremento presupuestario para ejecutar el plan. El presupuesto disponible en 2007 triplica el del 2004.

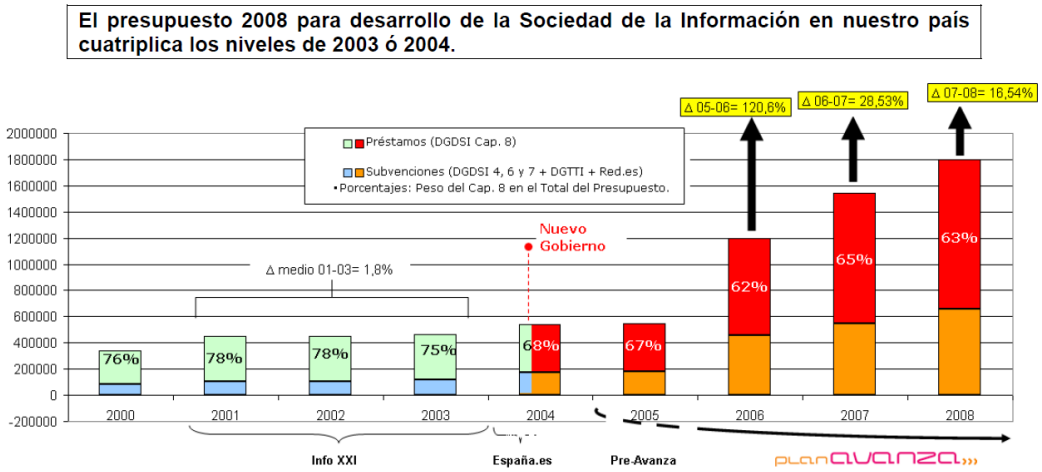


Figura 35 Presupuesto 2008 para desarrollo Sociedad de la Información

(Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2008)

Gran parte del presupuestario se dirige a la expansión de las redes de conexión a Internet, telefonía móvil, creación de telecentros para llevar conexión a Internet a las zonas rurales y periféricas para romper la llamada brecha digital, de la televisión digital terrestre, etc., lo que facilita, en los años venideros que se incremente el número de personas que acceden a las tecnologías de la información de la información y la comunicación.

De las áreas y medidas establecidas vamos a centrarnos en las que tienen mayor incidencia en el objeto de la investigación.

Impulsar el despliegue de infraestructuras, el desarrollo de servicios y la innovación.

En éste apartado, el Plan Avanza recoge iniciativas para impulsar la creación de contenidos digitales en España, para lo que se ha puesto en marcha la Convocatoria de contenidos digitales y la de Centros de referencia.

En Diciembre de 2007 se realiza el primer 'Foro Internacional de la Industria de Contenidos Digitales', el FICOD, cuya celebración coincide con el Foro Internacional sobre Propiedad Intelectual en el Entorno Digital.

La convocatoria financia proyectos y actuaciones para el desarrollo de contenidos y servicios digitales de calidad dentro del marco del Plan Avanza. En ésta convocatoria fueron aprobados 45 proyectos dirigidos a la creación de (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2008):

- Contenidos para el ocio y la cultura.
- Redes Sociales
- Centros experimentales
- Contenidos para la promoción de la sociedad de la información.
- Contenidos para el sector público.
- Difusión de contenidos.

En la convocatoria de Centros de referencia se financiaron proyectos y actuaciones que fomentasen la creación, desarrollo y potenciación de centros de referencia para el desarrollo de la Sociedad de la información. Fueron aprobados 37 proyectos.

Facilitar la incorporación a la sociedad de la información: capacitación y confianza de los usuarios.

Las acciones desarrolladas en el apartado van dirigidas a la incorporación de las TIC en todos los ámbitos económicos y sociales, distinguiéndose cuatro tipos diferentes:

- Difusión
- Fomento
- Derechos de los usuarios, seguridad y confianza
- Formación.

En la *Difusión* se realizan campañas dirigidas a la sensibilización de la sociedad de las oportunidades que presentan las tecnologías de la información y comunicación, y de alfabetización digital. En las acciones de *Fomento* se facilita la adquisición de equipamientos básicos. Las actividades enroladas en *Seguridad y Confianza* tratan de eliminar la inseguridad que producen el uso de las TIC, combinándose acciones de información, de protección a los usuarios y de mejora de los mecanismos de seguridad. Por último, en *Formación* se incorporan acciones formativas en empresas y centros educativos para mejorar los conocimientos y uso de las TIC, y se fomenta la formación on line.

B.1 Derechos de los usuarios, seguridad y confianza

Las acciones encaminadas a satisfacer las necesidades detectadas en este apartado son diversas:

- Servicio universal de telecomunicaciones.

- Oficina de atención al usuario de telecomunicaciones.
- Nuevas normas sobre protección y garantía de los derechos de los usuarios.
- Nuevas normas sobre servicios de tarificación adicional.
- Nuevas normas sobre calidad de los servicios de telecomunicaciones.
- Control y vigilancia del nivel de las emisiones radioeléctricas.
- Inspección y régimen sancionador en materia de telecomunicaciones.
- Inspección y régimen sancionador en materia de Sociedad de la Información.
- Inspección y régimen sancionador en materia de contenidos de televisión y obligaciones de inversión.

INTECO

Las acciones que vamos a analizar a continuación aportan garantías y seguridad a todos los usuarios de las telecomunicaciones.

Oficina de atención al usuario de telecomunicaciones

De todas las acciones llevadas a cabo en éste periodo la *'Oficina de atención al usuario de telecomunicaciones'* abierta en el año 2005 tiene por objetivo asegurar las garantías de los usuarios de telecomunicaciones, poniendo a su disposición información sobre sus derechos, respondiendo a las consultas sobre los servicios contratados y atendiendo a las reclamaciones que surjan. A través de la oficina se detectó la necesidad de establecer la normativa en cuanto a las altas y bajas de compañías de telecomunicaciones en el que se establece el derecho de todo usuario a darse de baja con el único requisito de avisar al operador con una antelación de quince días, creándose el *'Reglamento sobre protección de los usuarios de telecomunicaciones'establecida* en el Real Decreto 424/2005, de 15 de abril.

Nuevas normas sobre protección y garantía de los derechos de los usuarios

Las necesidades detectadas en la oficina realzaron la necesidad de la regularización de los derechos del usuario en el uso de los servicios de telecomunicaciones y de proporcionar seguridad y confianza a los usuarios de Internet.

Además del Real Decreto anteriormente mencionado, se crea una nueva regulación sobre el procedimiento de resolución de reclamaciones y atención al cliente por operadores. Se adapta la regulación a los problemas que se han detectado, la contratación de servicios no solicitados y los cambios de operador. También, se regula la justificación documental, que añade la obligación al operador de enviar la documentación sobre reclamaciones recibidas o información aportada a los usuarios implicados, a fin de que exista constancia de los sucesos. Los cambios en la protección y garantía de los derechos de los usuarios se detallan a continuación (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2008, pág. 105):

Los operadores deberán disponer de atención al cliente que resuelva las quejas, reclamaciones y cualquier incidencia contractual que planteen los clientes.

Los operadores están obligados a comunicar al abonado el número de referencia de sus reclamaciones, quejas o incidencias, para que quede constancia de las mismas.

Se detalla el contenido mínimo que debe figurar en los contratos para cualquier servicio de comunicaciones electrónicas.

Cuando el abonado de telefonía fija o móvil no pueda disfrutar del servicio contratado por una causa del operador, éste deberá indemnizar al cliente.

Para facilitar el cambio de operador el cliente tiene derecho a dar por finalizado el contrato en cualquier momento, debiendo comunicárselo al operador con una antelación mínima de 15 días.

El operador deberá comunicar al abonado cualquier propuesta de modificación del contrato, con una antelación mínima de un mes.

Nuevas normas sobre servicios de tarificación adicional

Debido a la multitud de quejas y reclamaciones derivadas de la aplicación de tarifas adicionales a usuarios se busca mejorar la respuesta frente a fraudes y abusos de servicios de tarificación adicional que producen la pérdida de confianza, e incrementar la protección y garantía de los derechos de los usuarios. Para crear el marco jurídico de la protección se procede a (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2008):

Crear la Orden PRE/2410/2004, del 20 de Julio, y resolución SETSI del 15 de Septiembre del 2004 mediante las cuales se establece:

La obligación de los operadores de suministrar información en una locución de 20 segundos en la que se le informa al usuario del precio, tipo de servicio, etc., antes de comenzar la tarificación adicional.

Derecho de los abonados a desconectarse de servicios de tarificación adicional.

Los servicios considerados de ‘tarificación adicional más caros’ requieren solicitud firmada de los usuarios (cláusula opt-in).

Se establecen medidas para evitar que el usuario de Internet pueda ser redirigido a un servicio de tarificación adicional.

Los operadores están obligados a desglosar en la factura las tarifas correspondientes a un servicio de tarificación adicional.

Borrador de la Orden Ministerial sobre servicios de tarificación adicional de telefonía móvil.

Las nuevas medidas adoptadas sobre la tarificación adicional redujeron significativamente las quejas y reclamaciones de los usuarios pasando del 46,7% del total de reclamaciones recibidas en 2004 al 0,7% en 2007.

Anteriormente a la creación de la orden ministerial, los usuarios de las telecomunicaciones experimentaban la falta de protección, desinformación e inseguridad derivada de su uso, lo que se tradujo en los altos porcentajes de reclamaciones que se realizaron. Del mismo modo que en aquella etapa de la evolución de las telecomunicaciones, la llegada de Internet produjo inseguridad y abusos que se fueron frenando, cuyas consecuencias actualmente latentes, producen falta de seguridad de los usuarios de Internet.

Nuevas normas sobre calidad de los servicios de telecomunicaciones

El objeto de la acción es proporcionar seguridad y confianza a usuarios en el uso de las telecomunicaciones con información pública comparable sobre la calidad de los servicios que prestan los operadores de telefonía fija, móvil y de acceso a Internet. Con éste motivo se crean tres instrumentos:

El Real Decreto 424/2005 del que hemos hablado anteriormente.

La Orden ITC/912/2006 que regulan las condiciones relativas a la calidad de servicios de comunicaciones electrónicas.

El Real Decreto 776/2006 del 23 de Junio que modifica el reglamento con el objeto de garantizar el derecho de los usuarios de obtener una compensación económica en los casos de interrupción del servicio.

Estos cambios tienen repercusión inmediata sobre los usuarios y la calidad de los servicios que perciben:

Los usuarios tienen a su disposición la oferta de las diferentes operadoras y sus productos.

Garantizan niveles mínimos de calidad de los servicios contratados.

En caso de la degradación del servicio o averías importantes, las operadoras deben de informar al Ministerio de Industria, Turismo y Comercio.

Aseguran a los usuarios facturación libre de errores.

Inspección y régimen sancionador en materia de telecomunicaciones

Se encarga de verificar y garantizar que las medidas adoptadas en cuanto a la protección y garantía de los derechos de los usuarios y de la calidad de los servicios de telecomunicaciones percibidos son cumplidas, imponiéndose en caso contrario medidas correctoras o sancionadoras, según el caso.

Como dato, de 2004 a 2008 se impusieron sanciones por importe global de aproximadamente 23 millones de euros.

B.2 Formación

Las medidas tomadas en el área de *Formación* van dirigidas a diferentes estamentos de la sociedad con el fin de evitar la posible brecha digital.

Se dota de infraestructuras, conectividad, equipamiento multimedia y dispositivos con conexión a Internet a las escuelas, disminuyendo el número de alumnos por Ordenador conectado.

Además, se planifican acciones que faciliten la incorporación de las TIC en las PYMES mediante acciones de formación a empleados.

Con el fin de presentar un breve pantallazo sobre el impacto cuantitativo de las actuaciones desde el año 2004 al 2008 en cuanto al acceso a Internet, infraestructura tecnológicas desarrolladas y otras acciones de la misma índole, a continuación podemos ver una tabla resumen de esta etapa publicada por la '*Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información'*.

Nuevos Programas desde Mayo'04	MARZO 2008	OBJETIVO
Educación en la era digital		
Nuevos colegios con acceso a la Banda Ancha y con más y mejor equipo informático	> 20.000	> 20.000 (2008)
Nº de universitarios con nueva cobertura WiFi	1,2 millones	1,2 millones
% Colegios con Banda Ancha *(mayo'04: 69%)*	92%	100%
Nuevos equipos instalados en colegios[1]	93.215 PCs (17.325 portátiles) 11.638 proyectores 1.752 pizarras interactivas 10.147 periféricos 7.570 redes WiFi	-
Escolares beneficiados	> 5 millones 450.000 docentes	7 millones 500.000 doctes.
Ciudadanía digital		
Ciudadanos beneficiados por las nuevas campañas de alfabetización digital	> 5 millones	-
Préstamos otorgados	> 165.000 (>115.200 familias y >60.100 empresas)	-
Nº de telecentros *(mayo'04: 292)*	2.954	3.000 (2008)
Bibliotecas conectadas en red *(mayo'04: 76)*	2.478	2.500
Ciudadanos beneficiados por los nuevos puntos de acceso a la Red	> 6 millones	-
Trabajadores beneficiados de programas de formación on-line	> 300.000	-
Nuevas poblaciones con cobertura de B.A.	56.168	58.000
Nuevos municipios con cobertura de B.A.	5.548	5.850
Ciudadanos con nueva cobertura de B.A.	8.240.885	8,5 millones
Nuevas poblaciones con cobertura de T. móvil	4.302	4.959 (2007)
Ciudadanos con nueva y mejor cobertura de telefonía móvil	> 1 millón	1 millón (2007)
Creación de dos Centros Nacionales de Referencia en TIC (INTECO y CENATIC)	-	-

[1] Los programas sin objetivo final constan de actuaciones de impacto variable (por el importe medio de los préstamos solicitados, población participante en las localidades objetivo...).

Figura 36 Impacto cuantitativo de las actuaciones desde el año 2004 al 2008

(Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2008)

3.4 Plan avanza 2 (2011 – 2015)

El Consejo de Ministros aprobó el 16 de Julio de 2010 la estrategia creada por la *Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información* en la que se da continuidad al Plan Avanza proponiéndose nuevos desafíos adecuados a la Sociedad en Red.

En el informe publicado con las estrategias del Plan Avanza 2, del que hemos obtenido la información de éste apartado, podemos ver que tras la primera fase del Plan Avanza en la que se perseguía superar el retraso en el que se encontraba España respecto de la Unión Europea, especialmente tal y como hemos apreciado, en cobertura y conectividad, la estrategia previa en el Plan Avanza 2 que fue prevista para ejecutarse en el periodo 2011 – 2015, se centra en el desarrollo y uso de productos y servicios TIC avanzados.

España, siguiendo los objetivos de la Unión Europea, ve en las TIC una oportunidad que permitirá salir de la crisis más rápido y fortalecidos.

En esta etapa, se apuesta por fomentar la Sociedad de la Información y se considera que para beneficiar al desarrollo económico a través de las TIC es necesario que todas las personas con independencia de la edad, género, residencia o capacidad, conozcan los beneficios que las TIC pueden aportarle. De esta manera, se busca producir en la sociedad un cambio cultural que, a través de las oportunidades que presentan las TIC, repercuta en mejorar el bienestar social de la ciudadanía, la productividad del tejido empresarial y la competitividad del sector TIC en España.

El objetivo general del Plan Avanza 2, es contribuir a la recuperación económica de nuestro país gracias al uso generalizado e intensivo de las TIC. Debido a la profunda crisis que atraviesa nuestro país se ha visto en las TIC una luz hacia la que dirigirse que se espera suponga crecimiento y desarrollo económico. Se prevé que las TIC van a ser uno de los sectores económicos de mayor crecimiento en los próximos años a escala mundial. Para situarnos en el contexto y visión de las estrategias y objetivos en Europa y España, podemos apreciar en las Figuras 37 y 38 el crecimiento que van a experimentar las TIC y los beneficios que suponen su investigación y desarrollo.

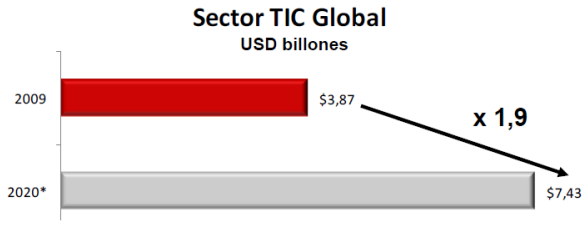


Figura 37 Crecimiento sector TIC

(Secretaría de estado de Telecomunicaciones y para la Sociedad de la Información, 2010a)

En España se prevé que el sector TIC se convertirá en el segundo sector generador de valor añadido bruto (VAB).

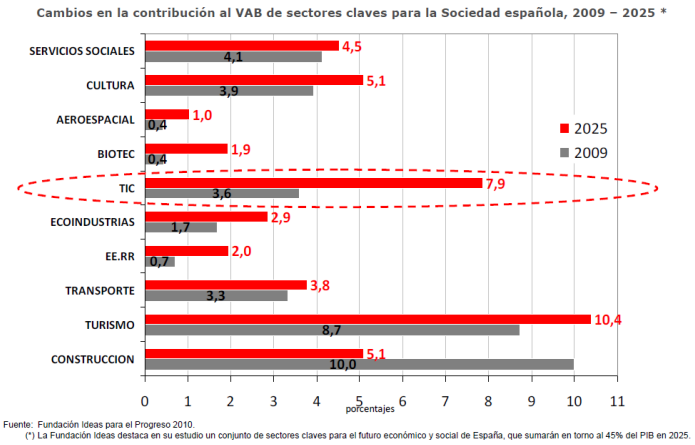


Figura 38 Cambios contribución VAB

(Secretaría de estado de Telecomunicaciones y para la Sociedad de la Información, 2010a)

Por ello, todos los expertos apuestan por un nuevo modelo productivo que refuerce la innovación, el conocimiento y el capital humano como dimensiones centrales de la crisis.

El crecimiento que se contempla no sería posible si las TIC no gozasen de la confianza y seguridad del consumidor, es decir, del usuario de Internet que como hemos empezado diciendo en el apartado lo integran personas de todas las edades, sexo o capacidades. El Plan Avanza 2 se divide en 4 bloques temáticos que contienen 10 objetivos concretos con los que se satisface el objetivo principal anteriormente mencionando (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2010b):

- Consecución de una administración sin papeles en el año 2015
- Promover procesos innovadores TIC en las Administraciones Públicas.
- Extender las TIC en la sanidad y el bienestar social.
- Potenciar la aplicación de las TIC al sistema educativo y formativo.

- Infraestructuras de telecomunicaciones
- Mejorar la capacidad y la extensión de las redes de telecomunicaciones.
- Uso y confianza en Internet: Una apuesta por la innovación.
- Extender la cultura de la seguridad de la información entre la ciudadanía y las empresas.
- Incrementar el uso avanzado de servicios digitales por la ciudadanía, participación en redes sociales, comunidades virtuales, comercio electrónico y utilización de la identidad digital.
- Extender el uso de soluciones TIC de negocio en la empresa.
- Impulso de la industria TIC española en sectores estratégicos.
- Desarrollar las capacidades tecnológicas del sector TIC.
- Fortalecer el sector de contenidos digitales.
- Desarrollar las TIC verdes, al constituir las TIC un instrumento clave para un crecimiento equilibrado desde la óptica medioambiental.

Únicamente vamos a desarrollar los subobjetivos que, a priori, pueden desprender acciones relacionadas con la seguridad en el uso de las TIC.

Uso y confianza en Internet: Una apuesta por la innovación

Extender la cultura de la seguridad de la información entre la ciudadanía y las empresas (Secretaría de estado de Telecomunicaciones y para la Sociedad de la Información, 2010a, pág. 9).

La generación de confianza es fundamental para el desarrollo de las TIC en todos los sectores productivos. Crear una cultura de seguridad en la que se garantice la

protección de los datos de los usuarios constituye un pilar fundamental para el desarrollo de la Sociedad de la información.

El Plan Avanza 2 considera que se deben combinar políticas públicas que velen por los derechos de los consumidores de Internet, ya sean niños, jóvenes o personas de la tercera edad, garantizando la protección sus datos e intimidad.

En este objetivo se insta a consolidar a INTECO como centro de excelencia y soporte al ciudadano en materia de confianza en la Sociedad de la Información.

En el año 2008, la incidencia de virus informáticos afectaba a un 58,2% de los internautas y el correo no deseado a un 49,5%, incrementándose significativamente los problemas en seguridad TIC. Sin embargo, en las empresas la tendencia es opuesta al del resto de los internautas de la red. Conscientes del riesgo que corren los equipos informáticos que no estén debidamente protegidos, han incorporado medidas de seguridad para evitar ser afectados por el creciente número de virus existentes en la red.

Además, se observa que es necesario promover la educación digital en materia de seguridad y privacidad en Internet, con el fin de que los usuarios se sientan más seguros y afianzados en el uso de las oportunidades que presenta Internet y de éste modo sean consumidores de recursos y servicios a través de la red. Las acciones que se plantean adoptar son las siguientes:

Realizar campañas para fomentar la confianza en las TIC entre ciudadanía y concienciación sobre la utilidad y la seguridad.

Financiar programas de sensibilización, planes de formación y centros de alerta para generar y reforzar la confianza en las TIC para fomentar el uso seguro de Internet.

Financiación de programas de alfabetización mediática.

Realizar programas de promoción de buenas prácticas para lograr un uso seguro y responsable de las TIC por parte de los menores de edad.

Diseño de estrategias para la resolución de incidencias que afecten a multitud de usuarios de Internet.

Gestionar la privacidad de forma equilibrada (Secretaría de estado de Telecomunicaciones y para la Sociedad de la Información, 2010a, pág. 11)

Las actividades que realizamos los usuarios de Internet en la red tienen impacto directo en la vida diaria de las personas, introduciendo comodidad y rapidez en el tratamiento de información, y en la privacidad de los propios usuarios. Por ello, la legislatura, desarrollada para este fin, busca proteger los derechos fundamentales de todos los ciudadanos y controlar el acceso y disposición de nuestros datos personales, a través de la Ley Orgánica de Protección de Datos, la Ley de Medidas de Impulso de la Sociedad de la Información y la Ley de Acceso Electrónico de los Ciudadanos a los servicios Públicos. De ellas, y del resto de las leyes que afectan y protegen a los usuarios de Internet hablaremos más adelante.

En el objetivo, se persigue el equilibro entre las posibilidades que ofrecen las TIC y las garantías de los derechos de los ciudadanos, considerándose clave la involucración de la industria y el establecimiento de una normativa adecuada. Las medidas establecidas son las siguientes:

Realizar campañas para fomentar que los prestadores de servicios utilicen servidores que alojen la información que dispongan de las medidas necesarias de

seguridad en el ámbito de aplicación de la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico.

Financiar proyectos de formación en el uso de las TIC con el fin de evitar prácticas de riesgo en el uso de las mismas.

Promover la adopción de planes de contingencia ante problemas de seguridad informáticos y de comunicaciones.

Elaborar guías para orientar sobre la aplicación práctica de las obligaciones legislativas, especialmente a las empresas que proporcionen bienes y servicios a través de la red.

Desarrollar servicios electrónicos que permitan a los ciudadanos conocer los datos de carácter personal suyos están a disposición de las administraciones públicas.

Incrementar el uso avanzado de servicios digitales por la ciudadanía, participación en redes sociales, comunidades virtuales, comercio electrónico y utilización de la identidad digital.

Para hacer posible este objetivo, es necesario que la población aprenda a utilizar las herramientas que se proponen y además, las utilice de manera segura sin exponerse a riesgos y conociendo las consecuencias de sus acciones en la red.

Por otro lado, este objetivo está especialmente dirigido a personas en riesgo de exclusión social para que puedan beneficiarse de la mejora del bienestar social y la promoción de igualdad social generado por las TIC.

Para el año 2015 se pretende que el 60% de la población utilice las redes sociales y el 50% realice compras on line.

Responsabilidad Plan Avanza

El seguimiento del Plan Avanza, correspondiente a la Oficina Técnica de Seguimiento del Plan Avanza, ha realizado análisis de su impacto en las áreas de actuación del Plan y ha elaborado documentación de seguimiento y evaluación.

La información de la ejecución del Plan Avanza proporcionada por la Oficina Técnica se complementa con los indicadores de impacto que elabora el Observatorio nacional de las Telecomunicaciones y la Sociedad de la información (ONTSI), que depende de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

Informe de Seguimiento Plan Avanza 2 (2013)

La estrategia del Plan Avanza 2 está alineada con la Agenda Digital para Europa de la cual hemos hablado con anterioridad y que fue aprobada por la Comisión Europea el 19 de Mayo de 2010, con objetivo es promover el desarrollo de la Sociedad de la Información y las TIC para la reactivación económica y la creación de empleo en la Unión Europea (Ministerio de Industria, Energía y Turismo, 2013b)

El mapa de proyectos puestos en marcha, facilitados en el informe de seguimiento de Septiembre de 2013 nos deja diferentes iniciativas en cada uno de los bloques temáticos del Plan Avanza 2:

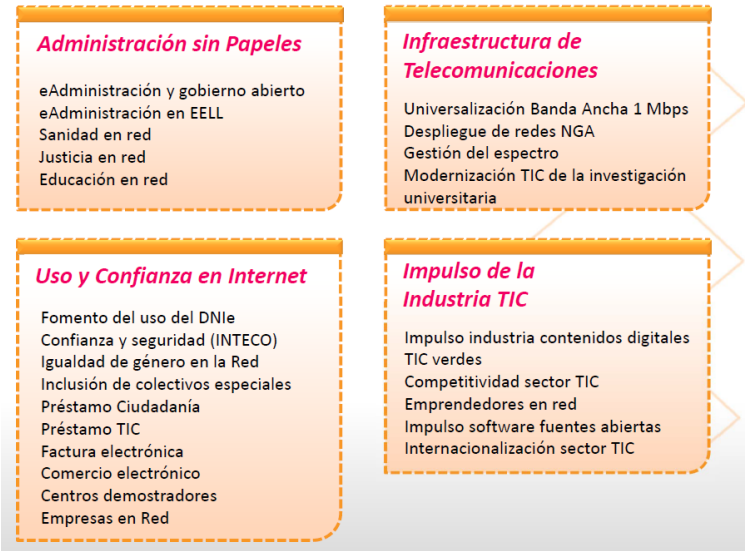


Figura 39 Iniciativas por bloques del Plan Avanza 2

(Secretaría de estado de Telecomunicaciones y para la Sociedad de la Información, 2010a)

Para ejecutar las medidas previstas han sido necesarios destinar los siguientes fondos a cada uno de los bloques (Ministerio de Industria, Energía y Turismo, 2013b):

Fondos Movilizados

(Miles de €)	Ejecutado 2006 - 2011			Presupuestado 2012			2006 - 2012		
Área	MITYC	Colaborador	Total	MITYC	Colaborador	Total	MITYC	Colaborador	Total
Administración sin papeles	706.095	565.045	1.271.140	45.888	0	45.888	751.983	565.045	1.317.028
Infraestructuras	1.050.127	303.197	1.353.324	27.685	0	27.685	1.077.812	303.197	1.381.009
Uso y Confianza en Internet	3.134.221	946.851	4.081.072	4.457	0	4.457	3.138.678	946.851	4.085.528
Impulso de la industria TIC	2.393.499	2.658.831	5.052.330	218.127	48.022	266.150	2.611.626	2.706.854	5.318.480
Otros	0	0	0	0	0	0	0	0	0
Total	7.283.942	4.473.923	11.757.866	296.157	48.022	344.180	7.580.100	4.521.946	12.102.045

Figura 40 Fondos movilizados

(Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2010b)

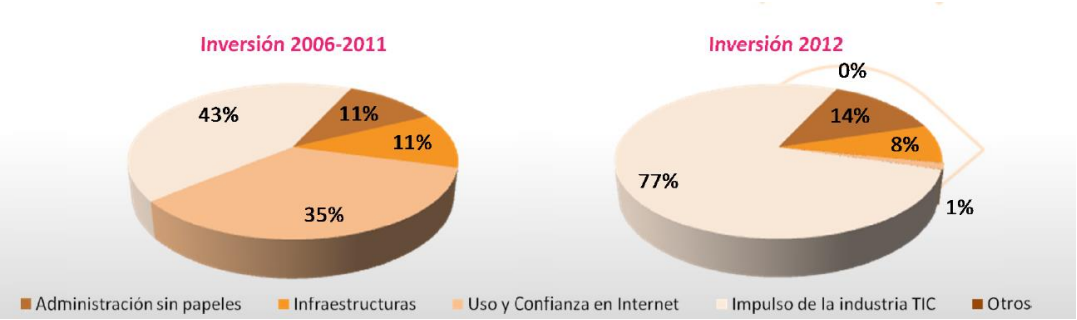


Figura 41 Comparativa de las inversiones

(Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2010b)

Podemos observar que en el periodo del 2006 – 2011 el '*Uso y Confianza en Internet'* fue el segundo bloque temático al que más fondos fueron dirigidos, mientras que en el año 2012 es el bloque temático al que menos fondos se dirigen. Hemos pasado de dirigir el 35% de los fondos al 1%.

Ante esta situación nos pueden surgir varias preguntas: ¿Han sido alcanzados todos los objetivos planteados para éste bloque temático que fueron planteados a finales del años 2010?, ¿Son los objetivos más intrascendentales de los planteados en el Plan Avanza 2?, y en definitiva, ¿Cuál es el motivo para que se invierta radicalmente la proporción de los fondos dirigidos a unos y otros bloques temáticos de objetivos?

El informe de seguimiento nos deja escasa información sobre el bloque de *Uso y Confianza en Internet,* prestando mayormente su atención en los fondos establecidos de los que hemos hablado, del porcentaje de hogares que tienen acceso a Internet, banda ancha y cuestiones relacionadas con las empresas y el volumen de mercado TIC.

Si nos observamos los fondos que se han dirigido por CCAA, prestando atención a la Comunidad de Madrid y por Municipios, Madrid, vemos que la situación es similar a lo ocurrido a nivel Español (Ministerio de Industria, Energía y turismo, 2013a).

Figura 42 Inversión Madrid

(Secretaría de estado de Telecomunicaciones y para la Sociedad de la Información, 2010a)

3.5 La Agenda Digital en España

"El Plan Avanza y su continuación, el Plan Avanza 2, fueron las estrategias del Gobierno en materia de Telecomunicaciones y Sociedad de la Información desde 2005 hasta la aprobación de la Agenda Digital para España el 15 de Febrero de 2013" (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2013)

Tras la aprobación el 15 de Febrero de 2013 de la Agenda Digital en España, la cual definiremos a continuación, se pone fin a ocho años de trabajo con el Plan Avanza y su sucesor el Plan Avanza 2, para adaptar los objetivos desarrollados hasta ese momento a los establecidos por la Agenda Digital para Europa e incorporando objetivos específicos para el desarrollo de la economía y la sociedad digital en España (Ministerio de Industria, Energía y Turismo, 2013).

La Agenda Digital en España 2013 – 2015 (ADpE)

El Ministerio de Industria, Energía y Turismo y el Ministerio de Hacienda y Administraciones Públicas han liderado la elaboración de la Agenda Digital para España, en sustitución de los plantes Avanza y su sucesor Avanza 2.

La Agenda Digital para España actuará como marco de referencia en el desarrollo de las tecnologías de la información y la comunicación en España, estableciendo la estrategia en nuestro país que nos permita alcanzar los objetivos de la Agenda Digital para Europa.

El propósito de la Agenda Digital busca favorecer la creación de oportunidades de empleo y el crecimiento económico, mediante una adopción inteligente de las tecnologías digitales que impulse la recuperación económica del país. Construir una sociedad inclusiva en la que toda la sociedad tenga los recursos y conocimientos para aprovechar los beneficios de las TIC, confíen en el comercio electrónico, utilicen la administración electrónica y tengan acceso de redes de banda ancha, se consideran necesarias para potenciar las oportunidades que presentan las TIC en el desarrollo económico del país. Para ello, se han establecido seis áreas de actuación la Agenda Digital para España en el periodo 2013 - 2015 (Ministerio de Industria, Energía y Turismo y Ministerio de Hacienda y Administraciones Públicas, 2013):

Fomentar el despliegue de redes y servicios para garantizar la conectividad digital y trasladar a la sociedad los beneficios económicos, sociales y de competitividad derivados de las redes de banda ancha ultrarrápida y del desarrollo de servicios digitales innovadores.

Desarrollar la economía digital para el crecimiento, la competitividad y la internacionalización de la empresa española mediante un uso más intenso y eficiente de las TIC, el fomento del comercio electrónico, el desarrollo de una industria de contenidos digitales, la internacionalización de la empresa tecnológica y la apuesta por las industrias de futuro.

Mejorar la e-Administración y adoptar soluciones digitales para una prestación eficiente de los servicios públicos mediante la transformación de la Administración.

Reforzar la confianza en el ámbito digital para fomentar el desarrollo de la actividad comercial, social y de relaciones entre ciudadanía, empresas y Administraciones a través de Internet.

Impulsar el sistema de I+D+i en Tecnologías de la Información y las Comunicaciones con el fin de alcanzar un crecimiento sostenible facilitando eficacia de las inversiones públicas y fomentando la inversión privada.

Promover la inclusión y alfabetización digital y la formación de nuevos profesionales TIC, fomentando la innovación y el emprendimiento, y facilitando la accesibilidad de todas las personas a los servicios y beneficios del ecosistema digital.

Algunos de los objetivos que se plantean son compartidos con la Agenda Digital para Europa, adaptados a la realidad de España, que nuestro país adopta con la convicción de que siguiendo esta dirección, España, estará preparada para competir en el ámbito internacional.

Para su puesta en marcha, la ADpE ha definido nueve planes específicos:

- Plan de telecomunicaciones y redes ultrarrápidas.
- Plan de TIC en PYME y comercio electrónico.
- Plan de impulso de la economía digital y los contenidos digitales.
- Plan de internacionalización de empresas tecnológicas.
- Plan de confianza en el ámbito digital.
- Plan de desarrollo e innovación del sector TIC.
- Plan de inclusión digital y empleabilidad.
- Plan de Acción de Administración Electrónica de la Administración General del Estado.
- Plan de servicios públicos digitales.

A continuación, examinaremos el plan que se va a desarrollar en la ADpE que afecta a nuestra investigación.

Plan de confianza en el ámbito digital 2013 – 2015 (PCAD). Agenda Digital para España

Las políticas de la Unión Europea, de los gobiernos más desarrollados en la OCDE y de España tienen plena confianza en un modelo centrado en la economía y las sociedades digitales para el crecimiento, el empleo y el bienestar.

La construcción de un clima de confianza se antoja imprescindible para satisfacer los objetivos propuestos, por lo que se requiere actuar sobre diferentes ámbitos como la ciberseguridad, la protección de la privacidad, el uso responsable y seguro de servicios y contenidos, la protección de colectivos vulnerables, la resistencia

y fortaleza de las infraestructuras tecnológicas y la seguridad jurídica que defienda nuestros derechos en las relaciones personales y económicas en Internet.

El plan de Confianza en el ámbito Digital (PCD) responde a la *Estrategia Europea de Ciberseguridad* (EUCS), que tiene por objeto favorecer que el ciberespacio sea abierto, seguro y protegido y que incluye iniciativas impulsadas por la Agencia Europea para la Seguridad de las Redes y de la Información (ENISA). También, responde a la Estrategia de Ciberseguridad Nacional (ESCN) del 2013 que trabaja para garantizar un uso seguro de las redes y los sistemas de información mediante la prevención, detección y dando respuesta a los ciberataques (Secretaria de Estado de las Telecomunicaciones y para la Sociedad de la Información, 2014).

El Plan de Confianza en el Ámbito Digital está compuesto por un conjunto de objetivos y políticas que pretenden cumplir los compromisos adquiridos en la Agenda Digital para España, en la Estrategia de Ciberseguridad Nacional y en la Estrategia Europea de Ciberseguridad. El PCAD ha dado lugar a un conjunto de medidas concretas organizadas por ejes que vamos a ver a continuación (Secretaria de Estado de las Telecomunicaciones y para la Sociedad de la Información, 2014).

El plan se divide en cinco ejes o áreas de actuación que dan lugar a un total de 25 medidas que prevén satisfacer los objetivos establecidos en los ejes.

Eje 1: Experiencia Digital Segura

Comprende las acciones encaminadas a sensibilizar, concienciar y formar en confianza digital.

Eje 2: Oportunidad para la industria TIC

Consta de un conjunto de acciones dirigidas a impulsar el desarrollo, mejorar la competitividad y ayudar a convertirse en referencia internacional en materia de confianza digital a la industria TIC.

Eje 3: Nuevo contexto regulatorio

Actuaciones regulatorias necesarias para afrontar el reto de construir una sociedad digital confiable, fomentando sus ventajas y respondiendo a los riesgos, bajo los principios de responsabilidad compartida y respeto de intereses y derechos de todas las partes.

Eje 4: Capacidades para la resiliencia: INTECO 2.0

En éste eje se planificará la transformación de INTECO para convertirlo en un centro de referencia en el mercado interior digital, centrado en la prevención, detección y respuesta ante incidentes de seguridad y a los compromisos de la Estrategia Europea y Nacional de Ciberseguridad.

Eje 5: Programa de Excelencia en Ciberseguridad (PECS)

Aprovechando la posición privilegia de INTECO, PECS generará una estructura de investigación especializada con la que fomentar la aparición, facilitar la identificación y la atracción del talento en materia de Ciberseguridad.

Con el fin de no desviarnos del objeto de nuestra investigación, a continuación examinamos las medidas que inciden mayormente sobre el objeto de la investigación.

Experiencia Digital Segura

Comprende las acciones encaminadas a sensibilizar, concienciar y formar en confianza digital.

Objetivos:

Realizar acciones de sensibilización, concienciación y formación orientadas a ciudadanos, empresas y colectivos vulnerables como infancia y adolescencia, para que conozcan las oportunidades que presentan los bienes y servicios TIC y adquieran confianza digital.

Explorar la viabilidad de incorporar contenidos sobre confianza digital en los itinerarios educativos.

Medidas:

Plan de sensibilización de INTECO. Actuaciones de sensibilización y mes de ciberseguridad.

Crear una plataforma de colaboración público-privada para incrementar la confianza digital que gestione las actuaciones de sensibilización, concienciación y formación, maximizando el impacto de las acciones. Además, tendrá como misión generar una cultura digital responsable que permita a ciudadanos y empresas disfrutar de las oportunidades de las TIC en un entorno seguro.

Se propone que la plataforma desarrolle las siguientes funciones:

Proponer, planificar y desarrollar acciones para la sensibilización y la formación de usuarios de Internet.

Elaboración de guías con recomendaciones y buenas prácticas en el uso de Internet.

Proponer mejoras para la protección de la infancia y la adolescencia y para la protección del consumidor on line.

Realizar actuaciones de sensibilización, concienciación y formación para la protección de la infancia y la adolescencia en Internet dentro del II Plan Estratégico Nacional de Infancia y Adolescencia 2013-2016, del Plan de Menores en Internet (medida 4) y en colaboración con el Plan de Contenidos Digitales y el Plan de Inclusión Digital y Empleabilidad de la Agenda Digital para España

Prueba piloto en itinerarios educativos escolares: se propone la puesta en marcha de una prueba piloto en los centros educativos que permita evaluar la eficacia de los contenidos específicos sobre seguridad, privacidad y uso responsable de las TIC que se realizan en los centros, y además, valorar la viabilidad de incorporar nuevos contenidos de confianza digital en los itinerarios educativos escolares.

Plan de menores en Internet: la propuesta reforzará el sitio web www.chaval.es, propone estudiar la viabilidad de un mecanismo que permita el etiquetado de contenidos digitales, del mismo modo que están haciendo las medidas vistas anteriormente impulsadas por la Comisión Europea, y promoverá la creación de un grupo de trabajo para la protección del menor donde estén implicados Ministerio de Interior (Guardia Civil, Policía), Fiscalía de Menores, Ministerio de Educación, Cultura y Deporte y el Ministerio de Sanidad Servicios Sociales e Igualdad junto a las CCAA. El grupo deberá recopilar y analizar las iniciativas realizadas, coordinando recursos y avanzando en la protección de los menores en Internet.

Las acciones que se planean llevar a cabo en el 'Plan de menores en Internet' son:

Crear una plataforma seguro con acciones divulgativas y preventivas. Ejemplo: www.chaval.es o www.menores.osi.es.

Desarrollar proyectos tecnológicos innovadores para la protección a la infancia y la adolescencia.

Fomentar acciones de sensibilización y formación dirigidas a profesorado, familias y jóvenes.

Estudiar el uso que hacen los jóvenes de Internet, los riesgos y situaciones dañinas a los que se exponen.

Punto Neutro de gestión de incidentes: se hará una prueba piloto para valorar la viabilidad de un centro neutro que coordine e implemente los protocolos de gestión de incidentes que se produzcan con los prestadores de servicios de la Sociedad de la Información. Además, se coordinará con proyectos internacionales de la misma naturaleza.

Podemos observar que las todas las medidas tomadas afectan directa o indirectamente a la seguridad con la que los jóvenes hacen uso de las TIC, bien porque las acciones conlleven labores de intervención con los jóvenes o, indirectamente, porque las medidas den lugar a un espacio virtual más seguro.

Informe de Seguimiento

En Noviembre de 2014 el Ministerio de Industria, Energía y Turismo, publicó un breve informe de seguimiento del Plan de Confianza en el ámbito Digital donde podemos apreciar los avances realizados desde el comiendo del mismo, reforzado y

ampliado por el informe anual de seguimiento de la ADpE publicado en Julio de 2015 (Ministerio de Industria, Energía y Turismo y Ministerio de Hacienda y Administraciones Públicas, 2015):

Participación en los procesos legislativos a nivel europeo sobre la Directiva de Seguridad de Redes y de la Información, el Reglamento de Identidad Electrónica y Servicios de Confianza y el Reglamento de Protección de Datos Personales.

Nuevo esquema de indicadores de confianza digital que ayude a detectar necesidades y demandas de servicios.

Se ha publicado un estudio sobre Ciberseguridad y Confianza en los hogares españoles, del que hablaremos más adelante.

Se ha visto necesario incrementar la sensibilización de ciudadanos y empresas sobre el uso responsable y seguro de Internet con el fin de reforzar las capacidades para la confianza digital.

Por éste motivo se están realizado actividades de sensibilización y difusión de uso seguro y responsable que tienen por objeto alcanzar a más de siete mil personas, prestando especial atención a los menores.

Se ha reforzado el INTECO, otorgándole mayor presupuesto, apoyo humano y material, así como una nueva dirección estratégica centrada en la ciberseguridad, pasándose a llamar Instituto Nacional de Ciberseguridad, INCIBE.

Se ha actualizado el currículo de secundaria con el RD 1105/2014, de 26 de diciembre, que examinaremos más adelante, por lo que ya no se ve necesario hacer la prueba piloto de itinerarios educativos escolares de la que hablamos anteriormente. Además, INCIBE, chaval.es y menores.osi.es ponen a disposición de jóvenes, familias, centro educativos y empresas contenidos en materia de seguridad en Internet.

Se ha puesto en marcha el punto neutro de gestión de incidentes de ciberseguridad y un servicio Antibotnet (mecanismo que reconoce amenazas o incidentes de cibersseguridad en las redes) en colaboración entre la Oficina de Seguridad al Internauta y las principales prestadoras de servicios de la sociedad de la información.

Se ha creado una nueva plataforma tecnológica que realice las funciones de alerta temprana de riesgos de seguridad y de vigilancia, y la protección de infraestructuras críticas a través de la cooperación con el CERT de Seguridad e Industria.

El seguimiento de los indicadores de la Agenda Digital ha sido realizado por el ONTSI. Los principales indicadores muestran que se ha aumentado el uso de software de seguridad situándose en el 62% de los usuarios, con respecto al 56% que los utilizaban en el año 2010. Sin embargo, el grado de confianza de los cibernautas se mantiene alrededor del 52%.

La ADpE ha creado el Foro Nacional para la Confianza Digital en el que participan 21 instituciones, que ha dado como resultado un nuevo eje de oportunidad para los profesionales de la ciberseguridad, dirigido a elaborar un marco de referencia, definir sus responsabilidades y revisar la oferta formativa en ciberseguridad del sistema educativo para proponer su adaptación a las nuevas necesidades.

Creación del Cibercamp 2014, que promociona el talento y la industria de la ciberseguridad, y realización de jornadas dirigidas a estimular el interés por la seguridad.

4. Otras iniciativas relevantes en la seguridad on line de los menores

4.1 eNACSO (European NGO Alliance for Child Safety On line)

Co-fundado por la Comisión Europea, eNACSO es una red compuesta por 27 organizaciones no gubernamentales de derechos de los niños en toda UE que tiene como objetivo "conseguir un entorno on line más seguro para los menores. Para ello promueven y apoyan acciones a nivel nacional y europeo para proteger a los menores y promover sus derechos en relación con Internet y las nuevas tecnologías" (INTEF, 2013).

Los objetivos de eNACSO se centran en las siguientes áreas (European NGO Alliance for Child Safety Online, 2014):

- La gobernanza de Internet y la protección infantil on line.
- La lucha contra el material de abuso sexual infantil on line.
- Identificación y protección de los niños víctimas de abuso sexual on line.
- Creación de medidas de protección y prevención dirigidas a los menores cuando están conectados a Internet.
- Fomentar los derechos y necesidades de los niños en las políticas gubernamentales.
- Acoso, manipulación y explotación sexual, a través de las TIC.

4.2 Protégeles

PROTÉGELES es una organización sin ánimo de lucro de protección al menor que inició sus actividades en 2002, en la que participan abogados, psicólogos y expertos en seguridad en seguridad en Internet. Las actividades que realizan van dirigidas a los jóvenes, centros educativos y familias, y siempre de forma gratuita.

PROTÉGELES es el 'Centro de Seguridad en Internet' para los menores, de referencia en España. El centro depende del programa Safer Internet Programme de la Comisión Europea. Como hemos visto anteriormente, PROTÉGELES es la única organización española miembro permanente del INHOPE (International Association of Internet Hotlines), del INSAFE (European network of Awareness Centers), y de Enacso (European NGO Alliance for Child Safety On line) (Asociación Protégeles, 2014).

Objetivos

Las actividades que desarrolla la fundación responden a la satisfacción de tres objetivos:

Facilitar a la policía y a la guardia civil el mayor número de informaciones verificables.

Mediante la denuncia de sitios web con contenidos ilícitos se pretende eliminar el mayor número de páginas de pornografía infantil en Internet, a nivel nacional e internacional.

Procurar la seguridad de los menores en el uso de las tecnologías de la información y la comunicación.

Para ello, se crean espacios dirigidos a los menores, con contenidos adaptados, donde se encuentran seguros. Además, se crean materiales didácticos, estudios relacionados con la seguridad en Internet, y se realizan campañas de prevención y formación dirigidas a jóvenes, padres y madres, y profesorado de centros educativos.

Desarrollar Líneas de ayuda profesionalizadas.

En los equipos se dispone de psicólogos, abogados y expertos de seguridad para dar respuesta a familias, menores y centros escolares sobre los riesgos derivados del uso de las TIC y siempre gratuitamente.

APP PROTEGETE

Tras el gran impacto de la utilización de las tecnologías móviles para conectarse a Internet, en 2012 PROTÉGELES junto a las operadoras de telefonía móvil (Telefónica, Vodafone, Orange y Yoigo), desarrollan una App para Smartphones con la funcionalidad de un botón de denuncia que permite, de manera fácil y rápida, enviar un informe de denuncia de los sitios web que contengan información ilícita o dañina para los menores.

4.3 Red.es

"Entidad pública empresarial adscrita al Ministerio de Industria, Energía y Turismo (MINETUR) que desarrolla un extenso conjunto de programas para que la sociedad española se beneficie al máximo de las posibilidades que ofrecen las TIC" (Minetur, 2002).

Nace en el año 2002, en el marco del Plan Info XXI en respuesta al proyecto e-Europe. La estructura profesional de Red.es ha ido evolucionando hasta conformar cuatro áreas de trabajo que podemos ver representadas en el siguiente diagrama:

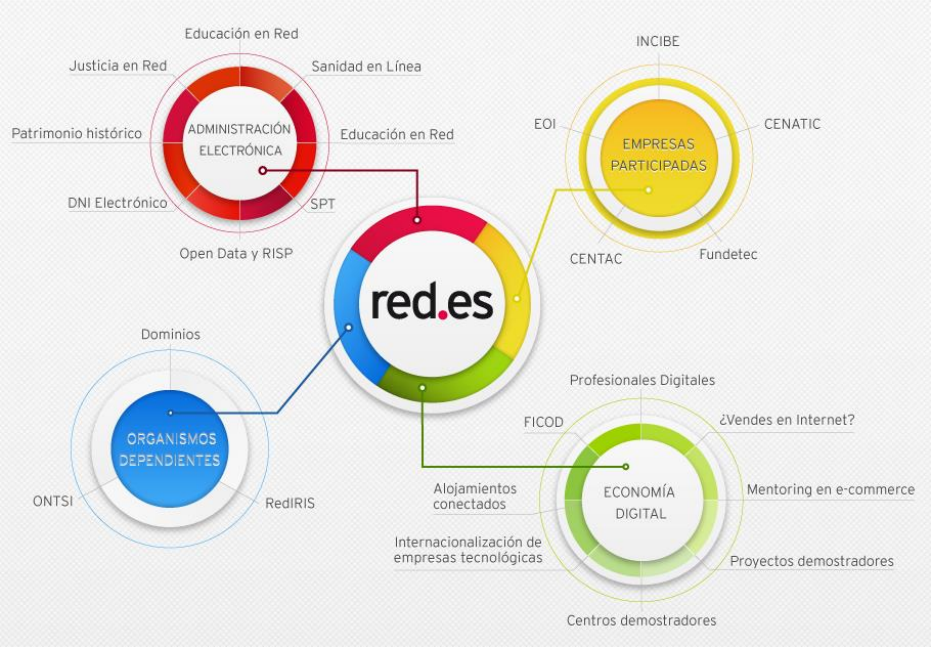


Figura 43 Áreas de trabajo Red.es

(Red.es, 2015a)

4.4 INTECO e INCIBE

El Instituto Nacional de Tecnologías de la Comunicación, INTECO, constituido en 2006, es una sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

INTECO fue concebido como instrumento de desarrollo de la Sociedad de la Información en España, encargado de gestionar, asesorar, promover y difundir

diferentes proyectos enmarcados en la estrategia del Gobierno contenida en el Plan avanza. Las áreas de actuación de INTECO son consideradas áreas de futuro en las que no existían experiencias previas desarrolladas en España.

A continuación, vamos a describir las líneas de actuación conferidas a INTECO en materia de seguridad en Internet.

Líneas de Seguridad Tecnológica

El objetivo de las Líneas de Seguridad Tecnológica es realizar labores de vigilancia, para detectar y evitar prácticas fraudulentas en la red. De este modo surgió la alianza de INTECO con el Centro de respuesta a incidencias de seguridad en TI, CERT que ha dado lugar a un conjunto de servicios preventivos en seguridad digital actuando como centro de referencia en que cuenta con recursos altamente cualificados.

En la misma línea fue creado el 'Centro Demostrador de Tecnologías de Seguridad' para las PYMEs que desarrolló un catálogo de productos, soluciones y servicios de seguridad, realizó además jornadas de sensibilización para PYMEs, etc.

Además, fue creado el *'Observatorio de la Seguridad'* que publica informes sobre el estado de la seguridad en Internet.

Proyectos desarrollado por INTECO

INTECO en colaboración con Red.es ha desarrollado proyectos sobre:

- Protocolo antifraude sobre dominios.es (phising)
- Campaña de Confianza en Red.
- Estudio sobre "Incidencia y confianza de los usuarios de Internet".
- Etc.

Tras la creación del Plan de confianza en el ámbito digital 2013 – 2015 (PCAD), de la Agenda Digital para España, se le asignó una nueva dirección estratégica centrada en la ciberseguridad, pasándose a denominar *Instituto Nacional de ciberseguridad (INCIBE)* que depende de Red.es

La actividad del INCIBE se apoya en tres pilares fundamentales (Instituto Nacional de Ciberseguridad de España, 2013):

Servicios: promueve servicios en el ámbito de la ciberseguridad que permitan el aprovechamiento de las TIC y eleven la confianza digital. Trabaja en la protección del usuario, fomenta el mecanismo para la prevención y reacción a incidentes de seguridad de información.

Investigación: realizan tareas de investigación en materia de ciberseguridad para la mejorar y mayor seguridad de los servicios.

Coordinación y colaboración con otras entidades, nacionales e internacionales, que permita dar una respuesta eficaz en el ámbito de la ciberseguridad.

4.5 Oficina de Seguridad del Internauta

La oficina de seguridad del internauta (OSI) depende de INCIBE y tiene el objetivo de reforzar la confianza en el ámbito digital a través de la formación en materia de ciberseguridad. Siguen tres líneas de trabajo (Oficina de Seguridad del Internauta, 2013):

- Ayudar a los usuarios a llevar a cabo un cambio positivo de comportamiento en relación con la adopción de buenos hábitos de seguridad.

- Sensibilizar a los usuarios de su responsabilidad en relación con la ciberseguridad.

- Contribuir a minimizar las incidencias de ciberseguridad de los usuarios.

Para ello ponen a disposición de los usuarios información sobre la seguridad en Internet, herramientas para navegar más seguro y realizan un boletín que difunden a través de un canal en el que todas las personas pueden inscribirse.

INTEF

"El Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado es la unidad del Ministerio de Educación, Cultura y Deporte responsable de la integración de las TIC en las etapas educativas no universitarias" (Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado, 2009)

Los objetivos principales del INTEF son (Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado, 2009):

- Elaboración y difusión de materiales curriculares y de formación para docente.
- Elaboración y difusión de materiales digitales dirigidos a su incorporación en las prácticas docentes para el beneficio del aprendizaje del alumnado.
- Colaboración con las CCAA para la elaboración de programas específicos en el ámbito de las TIC.
- Actualización del Portal de recursos educativos del Departamento y la creación de RRSS para facilitar el intercambio de experiencias y recursos entre el profesorado.

Organizaciones claves trabajando en el área de menores y TIC en ESPAÑA

Organismos Institucionales: Ministerio de educación, Consejerías de educación, Ministerio de Industria, Ministerio del interior (Guardia Civil, Policia). ONGs: Protégeles, Pantallas Amigas, y Alia2, son las principales ONGs operando a nivel nacional.

Es necesario resaltar que, además de las ONGs mencionadas, existen otro gran número de ONG realizando una gran labor en centros educativos de toda España a través de charlas y talleres de sensibilización en riesgos y oportunidades de las TIC para los jóvenes.

5. Ley orgánica para la mejora de la calidad educativa y real decreto por el que se establece el currículo de la enseñanza secundaria obligatoria

Las recomendaciones de la Comisión Europea a través de la Agenda Digital, destacando la acción 40 en la que se especifica la necesidad de que los centros educativos ofrezcan formación sobre seguridad en la red y alfabetización digital, y siguiendo las propuestas del eje 'Experiencia digital segura' del 'Plan de Confianza en el Ámbito Digital' perteneciente a la Agenda Digital para España, propiciaron la creación de la Ley Orgánica 8/2013, de 9 de diciembre, para la Mejora de la Calidad Educativa que incorpora y promociona las TIC en el sistema educativo español, y ésta a su vez, la reforma educativa de la Educación Secundaria Obligatoria en España.

Los principales objetivos que persigue la reforma educativa son reducir la tasa de abandono temprano de la educación, mejorar los resultados educativos de acuerdo con los criterios internacionales, mejorar la empleabilidad y estimular el espíritu emprendedor de los jóvenes.

Además, la LOMCE hace especial incidencia con vistas a la transformación del sistema educativo: las tecnologías de la información y la comunicación, el fomento del plurilingüismo, y la modernización de la Formación Profesional.

Ya desde su Preámbulo afirma que: Es necesario destacar tres ámbitos sobre los que la LOMCE hace especial incidencia con vistas a la transformación del sistema

educativo: las Tecnologías de la Información y la Comunicación, el fomento del plurilingüismo, y la modernización de la Formación Profesional.

La tecnología ha conformado históricamente la educación y la sigue conformando. El aprendizaje personalizado y su universalización como grandes retos de la transformación educativa, así como la satisfacción de los aprendizajes en competencias no cognitivas, la adquisición de actitudes y el aprender haciendo, demandan el uso intensivo de las tecnologías. Conectar con los hábitos y experiencias de las nuevas generaciones exige una revisión en profundidad de la noción de aula y de espacio educativo, solo posible desde una lectura amplia de la función educativa de las nuevas tecnologías.

La incorporación generalizada al sistema educativo de las Tecnologías de la Información y la Comunicación (TIC), que tendrán en cuenta los principios de diseño para todas las personas y accesibilidad universal, permitirá personalizar la educación y adaptarla a las necesidades y al ritmo de cada alumno o alumna. Por una parte, servirá para el refuerzo y apoyo en los casos de bajo rendimiento y, por otra, permitirá expandir sin limitaciones los conocimientos transmitidos en el aula. Los alumnos y alumnas con motivación podrán así acceder, de acuerdo con su capacidad, a los recursos educativos que ofrecen ya muchas instituciones en los planos nacional e internacional. Las Tecnologías de la Información y la Comunicación serán una pieza fundamental para producir el cambio metodológico que lleve a conseguir el objetivo de mejora de la calidad educativa. Asimismo, el uso responsable y ordenado de estas nuevas tecnologías por parte de los alumnos y alumnas debe estar presente en todo el sistema educativo. Las Tecnologías de la Información y la Comunicación serán también una herramienta clave en la formación del profesorado y en el aprendizaje de los ciudadanos a lo largo de la vida, al permitirles compatibilizar la formación con las obligaciones personales o laborales y, asimismo, lo serán en la gestión de los procesos. Es imprescindible, que el

profesorado adquiera los conocimientos necesarios para ser capaz de utilizar nuevas metodologías que mejores su actividad docente y la adquisición de conocimiento en el aula mediante las TIC (Egido, y otros, 2006).

Una vez valoradas experiencias anteriores, es imprescindible que el modelo de digitalización de la escuela por el que se opte resulte económicamente sostenible, y que se centre en la creación de un ecosistema digital de ámbito nacional que permita el normal desarrollo de las opciones de cada Administración educativa.

Además, en relación con las TIC, en la LOMCE se añade un nuevo artículo 111 bis con la siguiente redacción:

«Artículo 111 bis. Tecnologías de la Información y la Comunicación.

1. El Ministerio de Educación, Cultura y Deporte establecerá, previa consulta a las Comunidades Autónomas, los estándares que garanticen la interoperabilidad entre los distintos sistemas de información utilizados en el Sistema Educativo Español, en el marco del Esquema Nacional de Interoperabilidad previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Para ello, se identificarán los tipos básicos de sistemas de información utilizados por las Administraciones educativas, tanto para la gestión académica y administrativa como para el soporte al aprendizaje, y se determinarán las especificaciones técnicas básicas de los mismos y los distintos niveles de compatibilidad y seguridad en el tratamiento de los datos que deben alcanzar.

Dentro de estas especificaciones, se considerarán especialmente relevantes las definiciones de los protocolos y formatos para el intercambio de datos entre sistemas de información de las Administraciones educativas.

Estas medidas también irán encaminadas a potenciar y a facilitar el aprovechamiento de los registros administrativos en el marco de las estadísticas educativas estatales, para posibilitar la ampliación de la información estadística referida al alumnado, el profesorado, los centros y las gestiones educativas, lo que redundará en la mejora de las herramientas de análisis y de seguimiento de la actividad educativa y de las medidas de mejora de la calidad del Sistema Educativo Español.

2. Los entornos virtuales de aprendizaje que se empleen en los centros docentes sostenidos con fondos públicos facilitarán la aplicación de planes educativos específicos diseñados por los docentes para la consecución de objetivos concretos del currículo, y deberán contribuir a la extensión del concepto de aula en el tiempo y en el espacio. Por ello deberán, respetando los estándares de interoperabilidad, permitir a los alumnos y alumnas el acceso, desde cualquier sitio y en cualquier momento, a los entornos de aprendizaje disponibles en los centros docentes en los que estudien, teniendo en cuenta los principios de accesibilidad universal y diseño para todas las personas y con pleno respeto a lo dispuesto en la normativa aplicable en materia de propiedad intelectual.

3. El Ministerio de Educación, Cultura y Deporte establecerá, previa consulta a las Comunidades Autónomas, los formatos que deberán ser soportados por las herramientas y sistemas de soporte al aprendizaje en el ámbito de los contenidos educativos digitales públicos con el objeto de garantizar su uso, con independencia de la plataforma tecnológica en la que se alberguen.

4. El Ministerio de Educación, Cultura y Deporte ofrecerá plataformas digitales y tecnológicas de acceso a toda la comunidad educativa, que podrán incorporar recursos didácticos aportados por las Administraciones educativas y otros agentes para su uso compartido. Los recursos deberán ser seleccionados de acuerdo con parámetros de calidad metodológica, adopción de estándares abiertos y disponibilidad de fuentes que faciliten su difusión, adaptación, reutilización y redistribución y serán reconocidos como tales.

5. Se promoverá el uso, por parte de las Administraciones educativas y los equipos directivos de los centros, de las Tecnologías de la Información y la Comunicación en el aula, como medio didáctico apropiado y valioso para llevar a cabo las tareas de enseñanza y aprendizaje.

6. El Ministerio de Educación, Cultura y Deporte elaborará, previa consulta a las Comunidades Autónomas, un marco común de referencia de competencia digital docente que oriente la formación permanente del profesorado y facilite el desarrollo de una cultura digital en el aula.»

Las TIC en la Educación Secundaria Obligatoria

A continuación, examinaremos los elementos relativos a las tecnologías de la información y la comunicación y, más concretamente, aquellas asignaturas que incluyan formación e información sobre riesgos y hábitos seguros en Internet, que se han incluido según el Real Decreto 1105/2014, de 26 de diciembre, por el que se establece el currículo básico de la Educación Secundaria Obligatoria y del Bachillerato.

Las competencias básicas del currículo serán las siguientes:

- Comunicación lingüística.
- Competencia matemática y competencias básicas en ciencia y tecnología.
- Competencia digital.
- Aprender a aprender.
- Competencias sociales y cívicas.
- Sentido de iniciativa y espíritu emprendedor.
- Conciencia y expresiones culturales.

El RD además añade "Para una adquisición eficaz de las competencias y su integración efectiva en el currículo, deberán diseñarse actividades de aprendizaje integradas que permitan al alumnado avanzar hacia los resultados de aprendizaje de más de una competencia al mismo tiempo", es el caso de las tecnologías de la información y de la comunicación que son tratadas de manera transversal en el resto de asignaturas.

En las siete competencias básicas, tres de ellas son consideradas de mayor relevancia su pleno desarrollo. Es el caso de las competencias de Comunicación lingüística, Competencia matemática y competencias básicas en ciencias y tecnología.

El artículo 6 muestra los elementos transversales entre los que se encuentran las tecnologías de la información y la comunicación, independientemente de su tratamiento específico en algunas de las materias de cada etapa. Además, especifica que los currículos de Educación Secundaria Obligatoria y Bachillerato incorporarán elementos curriculares en los que se trate las situaciones de riesgo derivadas del uso inadecuado de las TIC.

El artículo 11 se especifican los objetivos de la Educación Secundaria Obligatoria y responsabiliza al centro educativo del desarrollo de las destrezas básicas que permitan a los jóvenes hacer un uso seguro y responsable de las tecnologías de la información y la comunicación.

En función de la programación de la oferta educativa que establezca la administración educativa, así como de la oferta de los centros educativos, los alumnos de primer ciclo de la ESO podrán cursar tecnología.

En la opción de enseñanzas aplicadas, es decir, en las orientadas a priori a la formación profesional, si así lo considera la administración educativa y el centro docente, tecnología, sería una asignatura troncal.

En cuarto de la ESO se podrá cursar la asignatura específica de Tecnologías de la Información y la Comunicación, si así es considerado.

Del mismo modo que en la ESO, en Bachillerato es considerado un objetivo prioritario que el alumnado desarrolle sus capacidades para utilizar con solvencia y responsabilidad las TIC, así como valorar de forma crítica las aportaciones de la tecnología a nuestras condiciones de vida.

En el primer y segundo curso de Bachillerato, según la Administración educativa y el centro de estudios, se podrá cursar Tecnologías de la Información y la Comunicación I y II respectivamente.

El uso de las tecnologías de la información y la comunicación es incluido de manera transversal en la mayor parte de las asignaturas. En algunas se exige para realizar tareas de indagación, búsqueda de información y exposición de trabajos, en

otras van un paso más allí y se analiza la aplicación y aportación de las TIC en su desarrollo.

Las asignaturas de tecnología y tecnologías de la información y la comunicación incluyen contenidos didácticos para aprender a hacer uso seguro y responsable de las tecnologías de la información y la comunicación, así como de las herramientas de comunicación.

El nuevo currículo da un paso hacia delante en la implicación y responsabilidad de los centros educativos en el uso seguro y responsable de las tecnologías de la información y la comunicación. Sin embargo, aún no podemos conocer los resultados de estos cambios. La correcta aplicación del nuevo currículo se enfrenta a dos dificultades principalmente, por un lado, la implementación de las leyes educativas depende de las Comunidades Autónomas y por otro lado las dificultades económicas que dificultan la correcta implementación de la Ley.

En el curso 2015/2016 se espera que el nuevo currículo sea incorporado, sin embargo, algunas comunidades autónomas ven complicado disponer del tiempo necesario para que esté preparado en el comienzo del curso. Concretamente siete CCAA aún no han aprobado sus decretos de ESO y Bachillerato a tres meses del nuevo curso:

- Andalucía
- Asturias
- Canarias
- Cataluña
- Murcia

- Navarra
- País Vasco

En cualquier caso, es necesario la supervisión y evaluación de la eficacia de las iniciativas tomadas desde el Ministerio de Educación, Cultura y Deporte para comprobar si la formación que reciben los jóvenes se traduce realmente en un uso seguro y responsable de las TIC.

6. Leyes y normativas españolas relativas a la seguridad en Internet

Desde que, a comienzos de siglo, comenzase a popularizarse el uso de Internet y las nuevas tecnologías el sistema jurídico español ha tenido que adaptarse a una nueva sociedad digital para poder dar respuesta a nuevos delitos surgidos, extendidos o agravados por el uso de las nuevas tecnologías.

Muchas de las normativas previas a la implantación de las nuevas tecnologías son extensibles al mundo digital, pero otras muchas han debido ser modificadas, ampliadas o incluso creadas otras nuevas para poder dar cobertura a la sociedad digital. Dado que las nuevas tecnologías son un campo en constante crecimiento, el sistema jurídico debe actualizarse en la misma medida en que se desarrolla Internet y sus posibilidades.

El número de normativas, leyes, decretos y otros textos legales relativos a este efecto a nivel local, autonómico, nacional e internacional son innumerables, por lo que a continuación se exponen solamente algunas de las más relevantes a nivel nacional.

Constitución Española, 1978

Ya en la norma suprema del ordenamiento jurídico español encontramos artículos relativos a la seguridad, la privacidad o la libertad. Sin duda, términos relativos a la seguridad en Internet de la que versa esta tesis.

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Mediante esta se ley se resalta la importancia de los derechos de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, ya descritos en la Constitución, dado su rango fundamental.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

El código penal aprobado en 1995 se ha visto obligado a introducir modificaciones que adapten su normativa, tipificando nuevos delitos relativos al uso de las nuevas tecnologías de la comunicación, siendo su última actualización el 28/0472015.

Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.

Esta ley supone el principal marco regulador de los derechos de los menores de edad, garantizándoles una protección uniforme en todo el territorio del Estado. Sin embargo, transcurridos casi veinte años desde su publicación, se han producido cambios sociales importantes que inciden en la situación de los menores y que demandan una mejora de los instrumentos de protección jurídica. Por lo que, recientemente, se ha presentado un "Proyecto de Ley de modificación del Sistema de Protección a la Infancia y a la Adolescencia".

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (Última modificación 2011)

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos

fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Respecto a los menores, dicha Ley establece que para poder prestar el consentimiento para el tratamiento de los datos de carácter personal se requiere la edad mínima de 14 años y, que en caso contrario, deben prestarlo los padres, tutores o representantes legales.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

El presente Real Decreto desarrolla la mencionada Ley Orgánica y establece la obligación de las empresas de poner en marcha diversas medidas destinadas a garantizar la protección de dichos datos, afectando a sistemas informáticos, archivos de soportes de almacenamiento personal, procedimientos operativos, etc.

Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

Esta Ley se aplicará para exigir la responsabilidad de las personas mayores de catorce años y menores de dieciocho por la comisión de hechos tipificados como delitos o faltas en el Código Penal o las leyes penales especiales.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Es objeto de la presente Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

Ley 59/2003, de 19 de diciembre, de firma electrónica.

Como respuesta a la necesidad de conferir seguridad a las comunicaciones por Internet surge, entre otros, la firma electrónica, regulada en la citada ley. La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

El objeto de este reglamento es la regulación de las condiciones para la prestación de servicios o la explotación de redes de comunicaciones electrónicas, en desarrollo del capítulo I del título II de la Ley 32/2003, de 3 de noviembre, General de

Telecomunicaciones, y de las obligaciones de servicio público y los derechos y obligaciones de carácter público aplicables en desarrollo del título III de dicha ley.

Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

Esta ley supone la adopción de una serie de iniciativas normativas dirigidas a eliminar las barreras existentes a la expansión y uso de las tecnologías de la información y de las comunicaciones y para garantizar los derechos de los ciudadanos en la nueva sociedad de la información.

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas.

Este real decreto tiene por objeto la aprobación de la Carta de derechos del usuario de los servicios de comunicaciones electrónicas, en desarrollo del artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual.

Esta Ley regula la comunicación audiovisual de cobertura estatal y establece las normas básicas en materia audiovisual sin perjuicio de las competencias reservadas a las Comunidades Autónomas y a los Entes Locales en sus respectivos ámbitos.

Ley 21/2014, de 4 de noviembre, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

El desarrollo de las nuevas tecnologías digitales de la información y de las redes informáticas descentralizadas han tenido un impacto extraordinario sobre los derechos de propiedad intelectual, que ha requerido un esfuerzo equivalente de la comunidad internacional y de la Unión Europea para proporcionar instrumentos eficaces que permitan la mejor protección de estos derechos legítimos, sin menoscabar el desarrollo de Internet, basado en gran parte en la libertad de los usuarios para aportar contenidos.

El vigente texto refundido de la Ley de Propiedad Intelectual, aprobado mediante Real Decreto Legislativo 1/1996, de 12 de abril, ha sido un instrumento esencial para la protección de estos derechos de autor, pero resulta cuestionable su capacidad para adaptarse satisfactoriamente a los cambios sociales, económicos y tecnológicos que se han venido produciendo en los últimos años. Por ello, se ha llevado a cabo una modificación del mismo que dé cobertura al impacto digital surgido del uso de las nuevas tecnologías.

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.

Según su Preámbulo, esta Ley tiene por objeto «la protección de personas y bienes y el mantenimiento de la tranquilidad ciudadana, e incluye un conjunto plural y diversificado de actuaciones, de distinta naturaleza y contenido, orientadas a una misma finalidad tuitiva del bien jurídico protegido». Dicha ley, incluye seguridad ciudadana a todos los niveles, incluidos entornos digitales.

Norma de Protección de datos que reconoce el "Derecho al Olvido"

El 13 de mayo de 2014 el Tribunal de Justicia de la Unión Europea dio la razón a un español que solicitó a Google que borrara de su motor de búsqueda los enlaces a sitios que contenían información que le perjudicaba, fallando a favor del 'derecho al olvido'.

En Junio del 2015, Bruselas aprueba la nueva norma de protección de datos que reconoce el 'derecho al olvido', que reconoce por primera vez el derecho de los ciudadanos a reclamar el borrado de información personal perjudicial y no pertinente de Internet. La norma para reforzar la protección de datos se ha debatido durante tres años. Se aplicará a Facebook o Google y prevé fuertes multas por incumplimiento. Se procesará información personal con el "consentimiento inequívoco" de los usuarios.

La nueva normativa tiene por objeto adaptar las reglas vigentes en la UE sobre protección de datos, que datan de 1995, a la nueva realidad de Internet y las redes sociales, garantizar un mayor control de los usuarios del tratamiento de sus datos personales en la red y reducir las cargas burocráticas para las empresas por un valor de unos 2.300 millones de euros anuales.

CAPÍTULO III. DISEÑO METODOLÓGICO

En éste capítulo se concreta, en primer lugar, el planteamiento del problema de investigación, donde veremos el objeto de estudio, los objetivos que se pretenden alcanzar, las hipótesis planteadas, las variables utilizadas, etc. Posteriormente, analizaremos el diseño de la investigación, el proceso de selección de la muestra y el procedimiento y analizaremos el instrumento de evaluación empleado. Finalmente, terminaremos examinando el plan de análisis propuesto teniendo en cuenta la naturaleza de los objetivos del estudio.

1. Planteamiento del problema de investigación

1.1. Objeto de estudio

Los niños y jóvenes, nativos digitales, han nacido inmersos en la Sociedad de la Información en la que participan activamente aprovechando al máximo sus posibilidades de comunicación y socialización (Instituto Nacional de Tecnologías de Información y la Comunicación, 2009). La integración de la tecnología en diferentes ámbitos de su vida ha facilitado el rápido aprendizaje del uso de dispositivos y software, sin embargo, esta rápida adquisición de conocimientos no ha evolucionado del mismo modo que la seguridad con la que los jóvenes utilizan las TIC (INTECO, 2009)

Debido a la constante evolución tecnológica, que ha dado lugar al nacimiento de oportunidades para los jóvenes en torno a las TIC, se han observado riesgos que podrían afectarles negativamente. Hasta el momento no se puede hablar de manera generalizada del daño que puede causar a un joven la exposición a alguno de dichos riesgos de la red,

ya que son múltiples los factores que intervienen en la afección del daño. Las consecuencias que tiene para un joven exponerse a los riesgos de la red difiere según el tipo de riesgo, de la persona y de las circunstancias que le rodean (Garmendia et al., 2011). Sin embargo, si es posible identificar factores de riesgos y analizar la exposición a los riesgos que experimentan los jóvenes.

Partiendo de las premisas recogidas en las investigaciones realizadas bajo el marco del programa Safer Internet de la Comisión Europea, destacando el proyecto EU Kids Online, y de los planes de actuación elaborados por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, se hace evidente la necesidad de crear estrategias que permitan hacer frente a los riesgos que derivan del uso de las TIC.

La presente investigación tiene por objeto el desarrollo de los hábitos seguros y responsables con los que los jóvenes hacen uso de las TIC, generando una base de conocimiento con las acciones desarrolladas por los actores implicados en su integración y desarrollo, que nos permita entender la situación actual del problema. En la primera etapa examinamos las políticas y programas generados en torno a la seguridad del usuario de las TIC, así como los principales estudios que visibilizan los hábitos de los jóvenes al utilizar las TIC. Posteriormente, se elaborará un instrumento que nos permita conocer los hábitos, delimitados en nuestra investigación, que actualmente tienen los jóvenes de 2º de la ESO al hacer uso de las TIC, que además permita establecer un punto de partida a futuras investigaciones. Finalmente, teniendo en cuenta toda la información recogida y una vez analizados los resultados obtenidos en

la fase del pretest, se desarrollará la estrategia de intervención que será implementada en el centro educativo seleccionado.

Los interrogantes que dieron lugar a la investigación, de los que hablaremos más adelante, son los siguientes:

- ¿Qué medidas han tomado los actores implicados para hacer frente a los riesgos surgidos con la evolución de las TIC?
- Las medidas tomadas, ¿consiguen erradicar la exposición a los riesgos que afectan a los jóvenes al utilizar las TIC?
- ¿A qué riesgos se exponen los jóvenes en la actualidad?
- ¿Qué efectos tiene un plan de intervención diseñado para desarrollar los hábitos seguros y responsables de los jóvenes al utilizar las TIC e implementado en el centro educativo?
- ¿Influye el género en los hábitos seguros y responsables de los jóvenes al hacer uso de las TIC?

1.2. Valoración del objeto de estudio

Pérez Juste (1990) plantea algunos criterios para analizar la resolubilidad y contrastabilidad del objeto de estudio que se presentan a continuación:

Criterio	Indicador
Real	¿Es nuevo el problema?

	¿Se dispone ya de una contestación al mismo?
Resoluble	¿Es este el tipo de problema que puede ser eficazmente resuelto mediante el proceso de investigación?
	¿Pueden ser recogidos datos relevantes para probar la teoría o encontrar respuesta al problema bajo consideración?
Relevante	¿Es el problema significativo?
	¿Se halla implicado en él un principio importante?
Factible	¿Tiene el equipo la necesaria competencia para realizar un estudio de este tipo?
	¿Conoce el equipo lo suficiente en este campo para comprender sus aspectos más importantes y para interpretar los hallazgos?
	¿Dispone el equipo de los conocimientos técnicos suficientes para recoger, analizar e interpretar los datos?
	¿Pueden obtenerse los datos pertinentes?
	¿Se dispone de sistemas o procedimientos de recogida de datos válidos y fiables?

	¿Se tienen los recursos económicos y humanos necesarios para llevar el trabajo?
	¿Hay posibilidades de conseguir una financiación?
	¿Se tiene el tiempo suficiente para finalizar el proyecto?
Generador	¿Produciría la solución algún avance en lo que se refiere a la teoría o la práctica?
	¿Va a abrir nuevos interrogantes en el campo de estudio?

El problema de la investigación es:

Real: si bien se han realizado estudios sobre los riesgos que experimentan los jóvenes al hacer uso de las TIC, no se ha dado con una solución satisfactoria que consiga erradicar la exposición a los riesgos de nuestros jóvenes. Se observa la necesidad de conocer los efectos de las intervenciones que se realizan con este propósito. Por ello, la estrategia de intervención elaborada pretender mejorar los hábitos seguros y responsables de los jóvenes disminuyendo su exposición a los riesgos derivados de las TIC. Además, podremos conocer los resultados obtenidos de la intervención desarrollada, sirviendo de precedente a futuras intervenciones. También es necesario tener en cuenta que, como hemos podido ver, los riesgos están en constante evolución por lo que se hace necesaria la realización de nuevas investigaciones que nos permitan conocer la situación actual del problema.

Resoluble: la metodología que se plantea, así como el instrumento elegido para la recogida de información, nos permite obtener todos los datos necesarios para dar respuesta a las preguntas que se plantean en la investigación.

Relevante: con el desarrollo de las TIC, los jóvenes hacen uso de ellas exponiéndose a riesgos cambiantes que les posiciona en situación de vulnerabilidad. Los riesgos, causantes de afecciones de distinta intensidad, pueden tener consecuencias muy graves, por lo que se hace necesaria su inmediata intervención.

Factible: únicamente se van a abordar los riesgos que, dado los conocimientos y capacidades del investigador y de la intervención, se puedan afrontar. En lo demás, el investigador tras años trabajando con colectivos en situación de vulnerabilidad, y más concretamente con menores, cuenta con los conocimientos necesarios para implementar correctamente la intervención propuesta. Además, se cuenta con la colaboración de los centros educativos donde se desarrollará la intervención, así como los recursos humanos, materiales, financieros y tecnológicos necesarios.

Generador: si bien existen investigaciones que nos muestran los hábitos de los jóvenes al hacer uso de las TIC, se hace necesario la identificación de estrategias de intervención que realmente produzcan que los jóvenes hagan uso de las TIC de forma responsable y segura. Mediante la presente investigación podremos analizar los resultados obtenidos en cuanto a dichos hábitos, antes y después de la intervención. Además, nos permitirá conocer el estado actual del problema y plantear nuevos caminos para continuar en un campo, que debido a los constantes cambios tecnológicos, se antoja desconocido.

1.3. Objetivos

El objetivo general de la presente investigación es:

Favorecer la adquisición de hábitos seguros y responsables en el desarrollo de la competencia digital, de los jóvenes de 2º de la ESO, que permita contrarrestar los riesgos y consecuencias nocivas que derivan del uso de las tecnologías de la información y la comunicación.

El objetivo planteado se desarrollará mediante la consecución de los siguientes objetivos específicos:

1. Examinar las principales políticas y programas, tanto nacionales como promovidos por la comisión europea, que favorezcan la seguridad con la que los jóvenes hacen uso de las TIC.
2. Implementar un plan de intervención que permita mejorar los hábitos seguros y responsables con la que los jóvenes hacen uso de las TIC.
3. Evaluar los efectos del plan de intervención diseñado, permitiéndonos conocer la exposición a los riesgos detectados.

1.4. Hipótesis

Las hipótesis tienen por finalidad ofrecer una explicación posible o provisional, teniendo en cuenta los sucesos y condiciones que toma en cuenta el investigador (Sabariego, 2004).

"Las hipótesis son proposiciones generalizadas o afirmaciones comprobables que se formulan como posibles soluciones al problema planteado" (Sabariego, 2004:128).

A partir de la experiencia de los programas y acciones examinadas en el marco teórico y de la experiencia previa en la intervención con jóvenes con el fin de mejorar los hábitos seguros en el uso de las TIC de la Fundación Balia y del propio investigador, se plantean las siguientes hipótesis:

Hp.1: Las medidas desarrolladas por los actores implicados en el desarrollo e integración de las TIC no eliminan la exposición a los riesgos derivados del uso de las TIC, que afectan a los jóvenes.

Hp.2: Los hábitos que actualmente tienen los jóvenes al hacer uso de las TIC les expone frente a los riesgos derivados de las mismas.

Hp.3: La implementación de un plan de intervención dirigido a desarrollar los hábitos seguros y responsables de los jóvenes disminuirá su exposición a los riesgos derivados del uso de las TIC.

Hp.4: La predisposición de los jóvenes a compartir información personal con personas conocidas a través de internet será menor tras la intervención.

Hp.5: La exposición a los riesgos derivados del uso de las TIC difiere según el género de los jóvenes.

Hp.6: La exposición a riesgos derivados del uso de las TIC de los jóvenes que han recibido información sobre hábitos seguros y responsables previamente a la intervención será menor que aquellos que no la han recibido.

1.5. Variables

Para el presente estudio se han considerado variables independientes (VI), definidas como aquellas que equivalen a la posible causa de los cambios observados al final del proceso de experimentación; variables dependientes (VD), que son aquellas que recogen los efectos o resultados que produce la variable independiente.

Variables Dependientes

Las variables dependientes responden al fenómeno que aparece, desaparece o cambia cuando el investigador aplica, suprime o modifica la variable o variables independientes (Sabariego y Bisquerra, 2004). En esta tesis, la variable dependiente es los 'Hábitos seguros y responsables de los jóvenes en el uso de las TIC', analizada en el alumnado de los centros participantes en el estudio, a través de 4 componentes que examinaremos más adelante:

- Hábitos de contacto: Engloba los hábitos y decisiones de los usuarios que permiten el acceso a sus redes sociales.
- Hábitos de contenidos: hábitos relacionados con la información que se comparte a través de internet.
- Hábitos de conducta: hábitos relacionados con la conducta de los usuarios con respecto a otros usuarios y páginas web.

- Hábitos de protección: medidas proteccionistas tomadas por los usuarios para proteger sus equipos informáticos.

Variables independientes

Las variables independientes son aquellas que el investigador manipula de manera deliberada para observar cómo influyen en la variable dependiente. En esta investigación hemos creado dos niveles de variables independientes:

- Variable independiente principal: la participación o no participación en el tratamiento. En nuestro caso, corresponde al centro educativo: IES Iturralde e IES García Morato, donde la muestra del grupo experimental corresponde con el alumnado del IES García Morato, mientras que la muestra del grupo de control corresponde al IES Iturralde.
- Variables independientes secundarias: el género e información recibida previamente sobre hábitos seguros y responsables en el uso de las TIC previamente al estudio.

La modalidad de intervención se definió por las condiciones de tratamiento en la investigación, que en este estudio fueron dos, la condición experimental y la condición control. La condición experimental se caracteriza por la participación del alumnado en un plan de intervención diseñado para dar respuesta a las necesidades que presentan los estudiantes, mientras que la condición control se refiere a la ausencia de participación en dicho plan. El alumnado participante en la condición experimental recibió un programa para el desarrollo de los hábitos seguros y responsables en el uso de las tecnologías de la información y la comunicación.

Como hemos podido ver a lo largo de la investigación, el género de los jóvenes es una variable significativa en la exposición a los riesgos derivados de las TIC, por lo que será analizada su influencia sobre la variable dependiente. La edad y el curso, no serán analizadas debido a que los grupos participantes en el estudio cursan 2º de la ESO, por lo que la diferencia de edad no se puede considerar relevante entre los alumnos participantes en el estudio. Por último, los padres, docentes e incluso actores externos al centro educativo pueden haber informado a los jóvenes participantes de los riesgos derivados del uso de las TIC previamente a nuestra llegada al centro educativo, por lo que se considera una variable que debe ser analizada por su posible influencia sobre los hábitos seguros y responsables de los jóvenes.

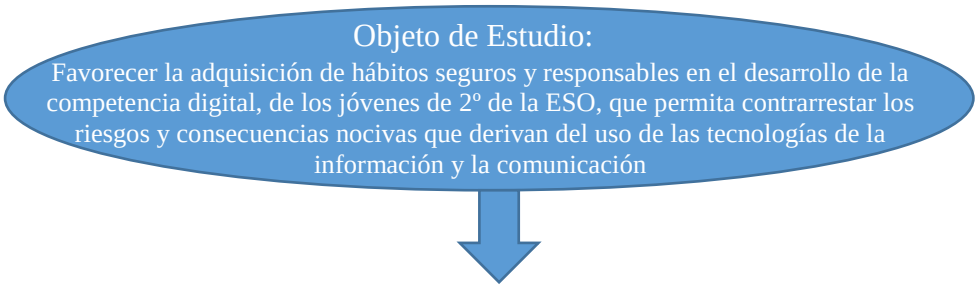
1.6. Formas de control de las variables: validez interna del experimento

En una investigación de corte experimental es fundamental evitar las fuentes de error que pueden afectar a los resultados y dotar de validez interna al experimento. Dos formas fundamentales de control que se han tenido en cuenta en esta investigación; el establecimiento de, al menos, un grupo de comparación o control y la asignación aleatoria de los participantes a las diferentes condiciones experimentales (Baker, 1997).

Se tuvieron en cuenta otras fuentes que afectan a la validez interna de un experimento como la historia, la instrumentación, la influencia del experimentador, la mortalidad muestral o la fidelidad del tratamiento (Campbell y Stanley, 1991). Respecto a la historia, el experimento se desarrolló con total normalidad, sin que existieran imprevistos que pudieran alterar los resultados finales. En cuanto a la instrumentación, se utilizó un instrumento fiable para evitar en los posibles fallos en la medición y que los resultados no se vieran afectados por sesgos atribuibles al instrumento. La

administración del cuestionario fue realizada por la misma persona para evitar sesgos entre los grupos. Además, se procuró evitar la mortalidad muestral o pérdida de sujetos en los grupos control y experimental al realizarse el experimento durante un espacio de tiempo concreto y reducido, en el transcurso del cual la mayor parte de los alumnos empezaron y terminaron el estudio.

En la Figura 44 *Figura 44 Resumen de investigación*se representan los aspectos principales que se han considerado para la investigación, con el objetivo de mostrar un resumen del presente estudio.



Hipótesis	
Las medidas desarrolladas por los actores implicados en el desarrollo e integración de las TIC no eliminan la exposición a los riesgos derivados del uso de las TIC, que afectan a los jóvenes.	
Los hábitos que actualmente tienen los jóvenes al hacer uso de las TIC les expone a los riesgos derivados de las mismas.	
La implementación de un plan de intervención dirigido a desarrollar los hábitos seguros y responsables de los jóvenes disminuirá su exposición a los riesgos derivados del uso de las TIC.	
La predisposición de los jóvenes a compartir información personal con personas conocidas a través de internet será menor tras la intervención.	
La exposición a los riesgos derivados del uso de las TIC difiere según el género de los jóvenes.	
La exposición a riesgos derivados del uso de las TIC de los jóvenes que han recibido información sobre hábitos seguros y responsables previamente a la intervención será menor que aquellos que no la han recibido.	
Muestra	
Jóvenes de 2º de la ESO	
Edad comprendida entre los 12 y los 16 años	IES García Morato IES Iturralde
Variables	
Variables Dependientes: Hábitos seguros y responsables en el uso de las TIC	
Variables Independientes: Modalidad de intervención, género, centro educativo e información previa recibida sobre hábitos seguros en internet	

Figura 44 Resumen de investigación

2. Diseño de la investigación

Los diseños cuasi-experimentales, principales instrumentos de trabajo dentro del ámbito aplicado, son esquemas de investigación no aleatorios. Dado la no aleatorización, no es posible establecer de forma exacta la equivalencia inicial de los grupos, como ocurre en los diseños experimentales. Cook y Campbell (1986) consideran los cuasi-experimentos como una alternativa a los experimentos de asignación aleatoria, en aquellas situaciones sociales donde se carece de pleno control experimental. Tal como afirma Campbell (1988), "podemos distinguir los cuasiexperimentos de los experimentos verdaderos por la ausencia de asignación aleatoria de las unidades a los tratamientos" (p. 191). Al interpretar los resultados de un cuasi-experimento, hay que considerar la posibilidad de que se deban a otros factores no tenidos en cuenta (Cook y Campbell, 1986).

El presente estudio se realiza mediante un diseño cuasi-experimental con grupo de control no equivalente (Campbell y Stanley, 1966), puesto que al tratarse de grupos de clases ya establecidas por el centro de enseñanza no se pudo respetar la aleatorización.

Dados los objetivos de este estudio, en la investigación se adoptó un enfoque cuantitativo que se caracteriza por ser explicativo, predictivo y de control, y cuyo objetivo principal es el de revelar por qué suceden los fenómenos a través de las evidencias observadas, la recopilación de datos y el análisis de los mismos. Los métodos cuantitativos utilizan procedimientos de medida fiables y válidos que proporcionan datos numéricos susceptibles de ser analizados a través de técnicas

estadísticas, con lo cual el investigador consigue que los resultados presenten objetividad (Bisquerra, 2004).

El diseño del plan de intervención para desarrollar los hábitos seguros y responsables de los jóvenes en el uso de las TIC se centró, en primer lugar, en la valoración de los resultados obtenidos en la administración del cuestionario pretest. Esto permitió detectar las carencias y necesidades de los jóvenes y elaborar un plan de intervención adaptado al grupo al que se dirige. Por último, la evaluación del efecto del programa de intervención se analizó en función de la modalidad de intervención.

Como se ha comentado con anterioridad, el diseño idóneo para la investigación es el diseño cuasi-experimental ya que, además, proporciona un control razonable sobre la mayor parte de las fuentes de invalidez. A pesar que no garantizan un nivel elevado de validez interna y externa como ocurre con los diseños experimentales, sí que ofrecen un grado de validez suficiente, por lo que suelen emplearse en las investigaciones educativas. Si bien el investigador en este tipo de diseño no puede hacer una asignación puramente al azar de los participantes a las condiciones experimentales, puede controlar cuándo llevar a cabo las observaciones, cuándo aplicar la intervención y cuáles de los grupos recibirá las diferentes modalidades de intervención.

Este diseño permitió establecer los efectos causales de las variables independientes sobre la variable dependiente y posibilitó un mayor control de las fuentes de validez interna. El investigador maneja al menos dos grupos de sujetos, ya establecidos, a los que administra un pretest, después suministra un tratamiento a uno de los grupos y, por último, administra el postest a ambos grupos, con la idea de comparar los resultados que nos permitan dar respuesta a las hipótesis planteadas.

Proceso de selección de la muestra

El tipo de muestreo utilizado es de tipo intencionado al tratarse de centros educativos en los que se permitió realizar el estudio. Además, el tamaño muestral es por conveniencia, tratándose de una muestra no representativa en la sociedad madrileña, sin embargo, nos permite sacar conclusiones significativas sobre la eficacia de la intervención.

La población objeto de estudio está formada por jóvenes que utilizan las TIC que actualmente cursan 2º de la educación secundaria obligatoria, con edades comprendidas entre los de 13 y los 16 años, residentes en el municipio de Madrid. Se eligieron los jóvenes de éste curso porque se consideran que son jóvenes que ya han adquirido unos hábitos en el uso de las TIC y aún se encuentran en pleno desarrollo de las competencias digitales.

La población participante está centrada en centros educativos públicos del área metropolitana de Madrid, los que la Fundación Balia por la Infancia tiene un convenio de colaboración y reúnen las características necesarias que se buscaban, concretamente centros educativos de la misma tipología, localizados en el mismo distrito, con características socioeconómicas y culturales similares. Los centros educativos que participan en el estudio son los siguientes:

- IES Iturralde: centro público situado en el barrio de Aluche, en el distrito de Latina.
- IES García Morato: centro público situado en el barrio de "Cuatro Vientos", en el distrito de Latina.

La Fundación Balia para la Infancia, que ha favorecido y apoyado el desarrollo del presente estudio, es una organización sin ánimo de lucro dedicada al desarrollo integral de la infancia y juventud en situación de riesgo, cuya misión es favorecer la inclusión social de menores en desventajas.

Como hemos visto la muestra proviene de diferentes contextos y se compone de personas (unidades):

Grupos de jóvenes participantes en el grupo experimental	
IES García Morato	62
Grupos de jóvenes participantes en el grupo de control	
IES Iturralde	45
Total Participantes en el estudio	
107	

3. Procedimiento

El desarrollo de la investigación está formado por cuatro fases claramente diferenciadas: la fase I, consistente en el establecimiento del problema y de los objetivos de investigación; la fase II, relativa al pretest o fase pre-experimental; la fase III (fase experimental), en la que se implementa el plan de intervención para el desarrollo de los hábitos seguros y responsables de los jóvenes al utilizar las TIC; la fase IV, correspondiente con el postest y la valoración del plan de intervención.

Para poder realizar el estudio, gracias a la colaboración de la Fundación Balia por la Infancia, que durante años ha desarrollado programas de intervención en centros educativos de la Comunidad de Madrid, Guadalajara y Sevilla, pudimos contactar con los equipos directivos de los centros educativos participantes. La experiencia y el apoyo de la Fundación Balia facilitaron enormemente la participación de los centros y el desarrollo de la intervención.

3.1 FASE I: establecimiento del problema y de los objetivos de la investigación

Esta primera fase se inicia con el establecimiento del problema y de los objetivos de la investigación. La investigación partió de la realidad observada en las aulas de centros educativos de la periferia de Madrid donde se detectó carencias en los hábitos seguros y responsables de los jóvenes cuando utilizaban las TIC, que dio lugar a experiencias negativas y afecciones percibidas por el alumnado. Además, verbalizaron la vulnerabilidad que experimentan cuando hacen uso de las TIC. Gracias a la realidad observada previamente en las aulas, a las características propias de la intervención y la

revisión literaria realizada se ha visto conveniente focalizar la intervención en los riesgos que se detallan más adelante.

En la fase I se establecieron una serie de cuestiones, vistas anteriormente, que mostraron el camino a seguir:

- ¿Qué medidas han tomado los actores implicados para hacer frente a los riesgos surgidos con la evolución de las TIC?
- Las medidas tomadas, ¿consiguen erradicar la exposición a los riesgos que afectan a los jóvenes al utilizar las TIC?
- ¿A qué riesgos se exponen los jóvenes en la actualidad?
- ¿Qué efectos tiene un plan de intervención diseñado para desarrollar los hábitos seguros y responsables de los jóvenes al utilizar las TIC e implementado en el centro educativo?
- ¿Influye el género en los hábitos seguros y responsables de los jóvenes al hacer uso de las TIC?

A partir de estas preguntas se establecieron los objetivos de la investigación para describir el fenómeno educativo estudiado desde un planteamiento riguroso y científico y, de este modo, tratar de valorar la contribución de un plan de intervención para el desarrollo de los hábitos seguros y responsables en el uso de las TIC.

- Introducción

Tras el surgimiento de estos interrogantes, el siguiente paso fue dar respuesta a la primera de las preguntas planteadas: ¿Qué medidas han tomado los actores implicados para hacer frente a los riesgos surgidos con la evolución de las TIC?

Con el fin de dotar a la investigación de un marco teórico-conceptual y científico se realizó una revisión de la literatura teórica y empírica, de lo más global a lo más cercano a la realidad que viven nuestros jóvenes. Se efectuaron múltiples búsquedas y lecturas bibliográficas, en inglés y español, con el fin de conocer los actores que están implicados directa o indirectamente en la exposición a los riesgos derivados del uso de las TIC que experimentan los jóvenes. Comenzando por la comisión europea y posteriormente en España, se pudo conocer los riesgos derivados de las TIC, las estrategias, los planes, los proyectos y las iniciativas dirigidas a hacer de internet un lugar más seguro para los jóvenes. Toda ésta revisión contribuyo a profundizar en el estado de la cuestión sobre el tema de estudio y así poder examinar aquella más relevante que nos permita conocer los caminos explorados, con el fin de comprender el lugar donde nos encontramos.

- Elección de la metodología

La metodología empleada en nuestro estudio fue condicionada por los objetivos planteados. Tras identificar el problema de investigación, se seleccionó el enfoque, la muestra participante, instrumentación, así como las técnicas de recogida de información y análisis que se consideraron más apropiadas.

3.2 FASE II: pretest

La fase pretest se inició con la administración de un cuestionario para evaluar los hábitos que tienen los jóvenes cuando utilizan las TIC, en el alumnado 2º de educación secundaria obligatoria, del grupo experimental y grupo control. La prueba fue administrada a un total de 62 alumnos del grupo experimental, más 45 alumnos del

grupo de control, que contaron con la participación de 3 y 2 líneas respectivamente. Todos los grupos de alumnos realizaron el pretest en el mes de Enero de 2015.

La administración de la prueba fue realizada por la misma persona con el fin de evitar sesgos involuntarios con alguno de los grupos. En la administración de la prueba se destacó la finalidad del mismo, la manera de responder las preguntas e incidiendo en el anonimato de los cuestionarios. Además, se explicó que los cuestionarios estaban numerados, siendo necesario que el alumno que cumplimentase un cuestionario con un número concreto, en la prueba postest tendría que cumplimentar el cuestionario que tuviese el mismo número. Los centros educativos por su parte gestionaron las autorizaciones del alumnado para formar parte del estudio. El tiempo empleado por el alumnado para responder los ítems del cuestionario fue de 15 minutos y durante su administración, no observaron dificultades en la comprensión de las preguntas al estar redactadas con un lenguaje claro, conciso y sin ambigüedades. El lugar elegido para la administración del cuestionario fue el aula de cada uno de los cursos participantes y la respuesta al mismo fue individual y voluntaria. Por otro lado, se acordó con los centros educativos que la intervención comenzaría en el mes de marzo, concretando las fechas de las sesiones en el periodo de tiempo pactado, que podemos ver en la Figura 45.

En el mes de Enero y Febrero, tras administrar el pretest, se procedió a analizar las respuestas obtenidas con el objetivo de conocer, más de cerca, la realidad del alumnado que formó parte del grupo experimental y asegurarse que los grupos eran equivalentes. En las respuestas a los cuestionarios se observó que, en general, los participantes habían adquirido hábitos que les exponían a los riesgos derivados del uso de las TIC. Sin embargo, la exposición en algunos de los riesgos analizados se producía

de manera desigual entre jóvenes de diferentes de distinto género. Además, la exposición a los riesgos es desigual, siendo especialmente alarmantes los relacionados con la exposición de información personal.

3.3 FASE III: planificación e implementación del plan de intervención

Las necesidades y carencias observadas en el alumnado en el pretest, sobre los hábitos seguros y responsables que han desarrollado al utilizar las TIC, fueron el punto de partida de la tercera fase. En primer lugar, se elaboró un plan de intervención centrado principalmente en los siguientes objetivos:

- Sensibilizar sobre los riesgos y oportunidades derivados de las TIC.
- Análisis conjunto sobre las consecuencias derivadas de las decisiones tomadas.
- Incidir en la responsabilidad del usuario de las TIC.
- Uso seguro y responsable de las TIC.

Se decidió que la intervención estaría compuesta por 2 sesiones, de 60 minutos cada una, en las que se utilizó una metodología activa y participativa. Durante el desarrollo de las sesiones se buscó en todo momento la provocación de los jóvenes para fomentar su participación, el debate y el análisis de experiencias vividas con las TIC. También, se incluyeron contenidos audiovisuales y se realizaron ejercicios grupales en los que se expuso a los jóvenes a diferentes situaciones que tuvieron que analizar de forma crítica cada uno de los grupos. Posteriormente, los grupos exponían sus conclusiones generándose un debate reflexivo y crítico. Los ejercicios se expusieron a través de presentaciones que ofrecen diferentes caminos que se pueden tomar, simbolizados con puertas numeradas, que abrimos posteriormente para que conocieran

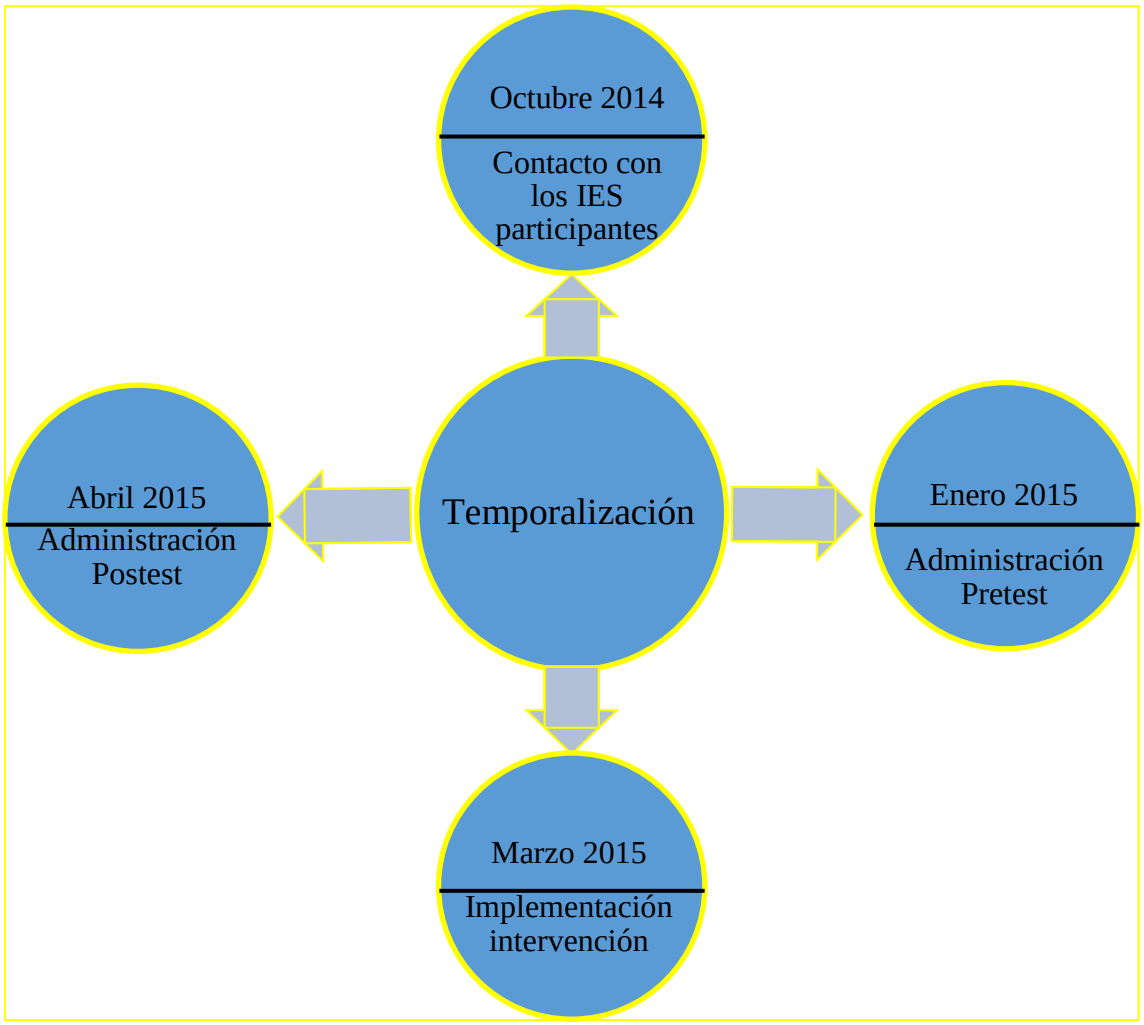
las consecuencias positivas y negativas de los otros caminos, cerrando un ciclo que podría terminar siendo una experiencia positiva o negativa.

TEMPORALIZACIÓN

El plan de intervención se implementó durante 4 meses, entre Enero y Abril de 2015, en el que cada grupo recibió un total de 2 sesiones de 60 minutos cada una. En la Figura 45 podemos apreciar el momento en que se produjo la intervención en cada uno de los centros educativos participantes.

CENTRO EDUCATIVO	**PRETEST**	**INTERVENCIÓN**	**POSTEST**
IES GARCÍA MORATO	ENERO	MARZO	ABRIL
IES ITURRALDE	ENERO	----------	ABRIL

Figura 45 Temporalización



3.4 FASE IV: postest

Una vez terminada la implementación de las sesiones, se dejó que trascurriese un mes con la intención que el postest estuviese condicionado lo menos posible por las percepciones de los jóvenes sobre respuestas correctas e incorrectas. Pasado éste periodo se suministró a los jóvenes el cuestionario postest, que consta de las mismas preguntas que el pretest a excepción de la pregunta 5 que sustituye a su homóloga, la pregunta 5 de pretest, para conocer los contenidos audiovisuales eliminados tras la intervención y la pregunta 9 que contempla las acciones realizadas por los jóvenes, tras

la intervención, en cuanto a la configuración de seguridad y privacidad de sus redes sociales.

Del mismo modo que ocurrió con el pretest, el cuestionario postest fue administrado por la misma persona que suministró el pretest.

En cuanto al análisis de los resultados se comprobó si los alumnos que formaron parte del grupo experimental (grupo que recibió el tratamiento) desarrollaron sus hábitos seguros y responsables al utilizar las TIC en mayor medida que aquellos que conformaron el grupo de control (grupo que no había recibido ningún tipo de intervención específica). Con ello, se pretendió determinar la idoneidad del programa para la mejora de esta capacidad en el alumnado. En este sentido, de acuerdo con Pérez Juste (2002), la evaluación de un programa permite conocer los resultados del mismo, potenciar sus efectos, rentabilizar los recursos y corregir los fallos, las disfunciones y las actuaciones inadecuadas detectadas en la implementación del programa.

4. Ética de la investigación

La ética de la investigación hace referencia al conjunto de normas y prácticas morales que el investigador debe tener en cuenta para la toma de decisiones en un estudio (Buendía y Berrocal, 2005). De acuerdo con la American Educational Research Association (1992), algunos de los principios éticos que deben considerarse en una investigación educativa son: (1) información de los objetivos del estudio, ya que es fundamental que los participantes conozcan el propósito de la investigación en la que colaboran; (2) privacidad, que implica el anonimato de los participantes y la confidencialidad por parte del investigador; (3) autonomía, que supone la expresión libre de ideas y opiniones de los participantes, sin presiones externas; y (4) cautela en la emisión de juicios, puesto que la falta de objetividad o el posicionamiento interesado del investigador afecta a la descripción del fenómeno estudiado.

En el caso de la metodología cuasi-experimental empleada en la presente tesis, además, las cuestiones éticas se relacionan con la asignación de los participantes a una u otra condición de tratamiento (experimental y control), ya que dicha asignación puede suponer ventajas o desventajas para el alumnado. Por este motivo, los participantes experimentan que se han visto más favorecidos que perjudicados por el estudio, para lo cual ha de salvaguardarse su privacidad, dignidad e intimidad.

5. Instrumentos de evaluación

Para la realización del presente estudio se ha elaborado un cuestionario que nos permite conocer los hábitos de los jóvenes, que se han considerado más relevantes, cuando utilizan las TIC. Además, en su elaboración se han tenido en cuenta las características del contexto madrileño y de la población a quien se dirige.

Con éste propósito, se realizó una revisión previa de la literatura sobre los riesgos derivados de las TIC a los que se exponen los jóvenes, así como sus causas y consecuencias. También, se analizaron las recomendaciones surgidas de los programas nacionales e internacionales que gozan de mayor validez, que han sido implementados hasta el momento de la intervención.

La elaboración del cuestionario constó de 3 fases. En la primera fase, tras su elaboración, se suministró a un grupo de jóvenes participantes en programas de la Fundación Balia con el fin de verificar la comprensión de las preguntas, que la información obtenida fuese la necesaria y que estuviesen ajustadas a la realidad de la exposición a riesgos de los jóvenes en el momento del estudio. Tras la primera fase se realizaron correcciones y se aplicó a otro grupo de jóvenes en lo que sería la segunda fase. Nuevamente, se procedió a realizar correcciones en el cuestionario y se aplicó el cuestionario en la tercera fase, dando con el instrumento adecuado para el estudio.

Los cuestionarios han sido validados por un grupo de 5 expertos, para dar un mayor nivel de fiabilidad a los resultados obtenidos, formado por un profesor de la Universidad Autónoma de Madrid, un profesor de la Universidad Europea, dos

profesores de la Universidad de Málaga y una experta en metodologías educativas en la integración de las TIC en el centro educativo.

Los instrumentos de evaluación utilizados son dos:

- Pretest: nos permite conocer los hábitos seguros y responsables de los jóvenes en el uso de las TIC antes de la implementación del plan de intervención.
- Postest: nos permite conocer los hábitos seguros y responsables de los jóvenes al utilizar las TIC, tras la intervención.

El conjunto del pretest y postest, nos permite medir el impacto de la intervención.

El pretest consta de 29 items que completan el cuestionario. Los ítems están distribuidos en 16 bloques de preguntas. Tras los 3 primeros ítems constan de preguntas de identificación, 2 preguntas cerradas politómicas, 15 preguntas dicotómicas, y 9 preguntas que utilizan una escala Likert de 1 a 5. Las preguntas que utilizan la escala Likert se responden según el grado de acuerdo con cada pregunta. Las alternativas que se han utilizado en las preguntas que utilizan la escala Likert son:

- Totalmente en desacuerdo;
- Bastante en desacuerdo;
- Ni acuerdo ni desacuerdo;
- Bastante de acuerdo;
- Totalmente de acuerdo

El cuestionario elaborado para la recogida de información en ésta fase, está compuesto por los siguientes ítems que se detalla a continuación.

Items cuestionario Pretest

Items		Valores
1	**Edad**	De 13 a 16 años
2	**Género**	1.Hombre 2.Mujer
3	**Centro educativo**	IES García Morato
		IES Iturralde
4	**Contactos en RRSS**	Amigos
		Amigos y amigos de amigos
		Amigos, amigos de amigos y a personas conocidas en internet
		A todo el mundo que me lo proponga
5	**Fotos personales en tus RRSS**	No tengo redes sociales
		Ninguna
		Entre 1 y 9
		Entre 10 y 50
		Entre 51 y 99
		Entre 100 y 200
		Más de 200
6	**Percepción fotos inadecuadas en RRSS**	1. Si / 2. No / 3. No tengo redes sociales

7	**Percepción comentarios inadecuados en RRSS**	1. Si / 2. No / 3. No tengo redes sociales
8	**Configuración seguridad y privacidad de las RRSS**	1. Si / 2. No / 3. No entiendo la pregunta
9, 10, 11	**Predisposición a compartir fotos o vídeos personales (amigos, amigos de amigos y conocidos en internet)**	1. Si / 2. No
12, 13	**Predisposición a compartir información con desconocidos (e-mail, nº de teléfono)**	1. Si / 2. No
14, 15, 16	**Predisposición uso de la webcam (amigos, amigos de amigos y conocidos en internet)**	1. Si / 2. No
17	**Humillación a terceros en RRSS**	1.Si/2.No/3.No tengo redes sociales
18, 19	**Uso de software de protección (ordenador de casa y Smartphone)**	1. Si / 2. No 3. No tengo ordenador en casa / Smartphone

20	**Valoración software de protección**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
21	**Predisposición al contacto con desconocidos a través del teléfono móvil**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
22	**Uso de páginas web adaptadas a la edad**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
23	**Percepción de seguridad en chats públicos**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
24	**Percepción delitos contra la propiedad intelectual**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
25	**Predisposición contacto con desconocidos a través de RRSS**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
26	**Estafas a través de la web**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
27	**Predisposición conocer en persona a usuarios conocidos en internet**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
28	**Percepción humillación online vs presencial**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)

29	**Información previa hábitos seguros y responsables**	1.Si/2.No

Figura 46 Items Pretest

El Postest consta de 30 ítems distribuidos en 17 bloques de preguntas. Tras los 3 primeros ítems, que constan de preguntas de identificación, el cuestionario contiene 16 preguntas cerradas dicotómicas, 1 pregunta cerrada politómica, 1 pregunta que utiliza una escala de intensidad y 9 preguntas que utilizan una escala Likert de 0 a 5 que pide que se califique según su grado de acuerdo con cada pregunta. Las alternativas que se han utilizado en las preguntas que utilizan la escala Likert son:

- Totalmente en desacuerdo
- Bastante en desacuerdo
- Ni acuerdo ni desacuerdo
- Bastante de acuerdo
- Totalmente de acuerdo

El cuestionario elaborado para la recogida en información tras la intervención, está compuesto por los ítems que se detallan a continuación.

Items cuestionario postest

Items		**Valores**
1	**Edad**	De 13 a 16 años
2	**Género**	1.Hombre 2.Mujer

3	**Centro educativo**	IES García Morato IES Iturralde
4	**Contactos en RRSS**	Amigos Amigos de amigos Conocidos por internet A todo el mundo que me lo proponga
5	**Fotos o vídeos eliminados tras la intervención en tus RRSS**	No tengo redes sociales Ninguna Pocas Algunas Bastantes Muchas
6	**Percepción fotos inadecuadas en RRSS**	1. Si / 2. No / 3. No tengo redes sociales
7	**Percepción comentarios inadecuados en RRSS**	1. Si / 2. No / 3. No tengo redes sociales
8	**Configuración seguridad y privacidad en RRSS**	1. Si / 2. No / 3. No entiendo la pregunta
9	**Revisión reciente de la configuración de seguridad y privacidad**	1.Si/2.No/3.No tengo redes sociales

10, 11, 12	**Predisposición a compartir fotos o vídeos personales (amigos, amigos de amigos y conocidos en internet)**	1. Si / 2. No
13, 14	**Predisposición a compartir información con desconocidos (e-mail, nº de teléfono)**	1. Si / 2. No
15, 16, 17	**Predisposición uso de la webcam (amigos, amigos de amigos y conocidos en internet)**	1. Si / 2. No
18	**Humillación a terceros en RRSS**	1.Si/2.No/3.No tengo redes sociales
19, 20	**Uso de software de protección (ordenador de casa y Smartphone)**	1. Si / 2. No 3. No tengo ordenador en casa / Smartphone
21	**Valoración software de protección**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
22	**Predisposición al contacto con desconocidos a través del teléfono móvil**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)

23	**Uso de páginas web adaptadas a la edad**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
24	**Percepción de seguridad en chats públicos**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
25	**Percepción delitos contra la propiedad intelectual**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
26	**Predisposición contacto con desconocidos a través de RRSS**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
27	**Estafas a través de la web**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
28	**Predisposición conocer en persona a usuarios conocidos en internet**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
29	**Percepción humillación online vs presencial**	Escala de valoración de 1 - 5. (1. Nada de acuerdo – 5. Totalmente de acuerdo)
30	**Información previa hábitos seguros y responsables**	1.Si/2.No

Figura 47 Items Postest

Justificación de las variables utilizadas en el estudio

Las preguntas incluidas en los cuestionarios nos permiten recoger información sobre los hábitos de los jóvenes que les exponen a los riesgos incluidos en el estudio que derivan del uso de las TIC. A continuación, se examinará la justificación de las variables que forman parte del estudio que nos permiten recoger la información necesaria para su posterior análisis:

- Edad: hemos podido comprobar, a lo largo de la investigación, que la edad es una variable significativa en el estudio de la exposición a los riesgos que forman parte del estudio. Sin embargo, al tratarse de personas que realizan el mismo curso académico, salvo excepciones de las personas que han repetido, la diferencia de edad es circunstancial dado que han nacido en el mismo año e irán igualando su edad en los meses venideros.
- Género: en estudios previos se ha demostrado que el género es una variable significativa en la exposición a riesgos derivados de las TIC. Los hombres y mujeres se exponen a unos u otros riesgos de manera desigual. Además, en estudios sobre la percepción del daño en la exposición a riesgos también se observan claras diferencias en función del género (Garmendia et al., 2011). Por estos motivos, se analizará la influencia de la variable género en los hábitos adquiridos por los jóvenes.
- Centro educativo: es una variable identificativa que se utilizará para distinguir al grupo experimental del grupo de control. ubicado en distintos barrios de un mismo distrito.

- Contactos en redes sociales: los jóvenes, al hacer uso de las redes sociales, deciden las personas que pueden acceder a su información compartida, aceptando, previamente, el acceso a su red social. Las personas que los jóvenes aceptan en sus redes sociales pueden ser muy cercanas, como familiares, compañeros del instituto, del equipo deportivo, etc., o pueden tratarse de personas desconocidas que le han enviado una 'solicitud de amistad' a través de una red social.
- Fotos personales en RRSS: A través de las aplicaciones de redes sociales se pueden compartir todo tipo de información digital: opiniones y comentarios, imágenes, audios, vídeos, etc. La exposición de información personal es uno de los principales factores de riesgo desencadenantes de la exposición a los riesgos que derivan de las TIC. Conocer la cantidad y calidad, según la percepción de los jóvenes, se antoja necesario para realizar actividades de prevención con los grupos.
- Percepción fotos inadecuadas en RRSS: percepción que tienen los jóvenes de la valoración de sus progenitores sobre los fotos que tienen compartidas. Ésta pregunta nos aporta información sobre la calidad de la información compartida.
- Percepción comentarios inadecuados en RRSS: percepción que tienen los jóvenes de la valoración de sus progenitores sobre los comentarios que tienen publicadas. Ésta pregunta nos aporta información sobre la calidad de la información compartida.
- Configuración seguridad y privacidad de las RRSS: Una de las medidas principales para controlar las personas que tienen acceso a la información, que el usuario comparte a través de sus redes sociales, es la configuración de

privacidad y seguridad de la misma. Cuando un usuario se crea una cuenta en una aplicación de red social se le asigna la configuración básica y general de la aplicación, dirigida a satisfacer los intereses de la empresa propietaria. Sin embargo, el usuario puede configurar algunos parámetros de la privacidad según sus propios intereses. En la intervención, se pretenderá incrementar el interés de los usuarios a ser ellos mismos quienes configuren las opciones de seguridad y privacidad de las redes sociales que utilizan.

- Predisposición compartir fotos o vídeos personales, según proximidad: La exposición a riesgos depende no sólo de la información compartida sino también de las personas que tienen acceso a la información. En ésta pregunta podremos conocer la intención de los jóvenes en compartir información audiovisual con las personas especificadas, según el grado de proximidad al joven.
- Predisposición a compartir información con desconocidos: compartir información personal con personas conocidas en la web constituye un factor de riesgo que expone al joven a múltiples riesgos derivados del contacto con desconocidos. En este caso, se pretende conocer la intención de los jóvenes a compartir la información especificada con personas conocidas a través de internet.
- Predisposición uso de la webcam: El uso de la webcam puede suponer un factor de riesgo grave, dependiendo de las personas con las que realice la actividad que puede derivar en otros peligros como el ciberbullying, sextorsión, etc. Por ello, recogemos información sobre la intención de los jóvenes a usar la webcam con diferentes personas según el grado de cercanía al joven.

- Humillaciones a terceros a través de RRSS: los jóvenes deben conocer los efectos que producen las burlas y humillaciones a través de las redes sociales en otras personas. La sensibilización en éste ámbito se antoja imprescindible para combatir el acoso online. Por éste motivo, se han incluido 2 items que nos permitirán conocer la percepción de los jóvenes sobre la humillación online en comparación con la humillación en persona y aquellos que se han burlado de fotos o comentarios en redes sociales.
- Uso de software de protección: El uso de antivirus, firewall y otras aplicaciones, protegen al usuario de intrusiones indeseadas en sus dispositivos de conexión a internet, que puedan acceder a su información personal. En ocasiones, información extraída con técnicas tan sofisticadas como éstas, es utilizada para chantajear a los usuarios de internet.
- Valoración software de protección: Los participantes podrán valorar la importancia del software de protección.
- Predisposición al contacto con desconocidos a través del teléfono móvil: A través de aplicaciones que permiten contactar con personas desconocidas pueden establecerse relaciones que generen confianza en los usuarios. El riesgo de no conocer en persona, previamente, a los usuarios conocidos en internet y generar confianza hacia ellos tiene el riesgo de compartir información personal, y por ende, de exponerse a todos los riesgos que derivan de ésta situación. En ésta variable se pretende medir la predisposición de los jóvenes a compartir el número de teléfono móvil personal con personas que han conocido en internet, con las que han generado una relación de confianza.

- Uso de páginas web adaptadas a la edad: El acceso a páginas web no adaptadas a la edad de los jóvenes les expone a visualizar contenidos inadecuados que pueden dañarles. Por éste motivo, nos interesa conocer si los jóvenes acceden, únicamente, a páginas adaptadas a su edad o si por el contrario, acceden a cualquier página disponible.
- Percepción de seguridad en chats públicos: El acceso aplicaciones web cuya funcionalidad principal es facilitar el contacto entre personas desconocidas, supone la exposición a los riesgos derivados del contacto con desconocidos que se han visto en el marco teórico. A través, de éste ítem podremos conocer la percepción de los jóvenes sobre seguridad en los chats públicos.
- Percepción delitos contra la propiedad intelectual: La descarga de material con derechos de autor supone el acceso a páginas web que incumplen la normativa realizando infracciones de derechos de autor. La participación en éste acto ilegal debe ser conocida y comprendida por los jóvenes, ya las acciones que realicen con el contenido descargado ilegalmente pueden suponer infracciones de derechos de autor (Ministerio de educación, cultura y deporte, 2015). Además, las páginas que facilitan las descargas ilegales, suelen contener software malintencionado y contenidos inadecuados.
- Predisposición contacto con desconocidos a través de RRSS: el acceso de personas conocidas a través de internet, a las redes sociales de los jóvenes supone la exposición a todos los riesgos derivados del contacto con desconocidos. Además, de dar acceso a toda la información compartida hasta el momento, se puede dar acceso a información personal de manera inintencionada que sea compartida en adelante.

- Estafas a través de la web: Un modo habitual de engaño utilizado en páginas web, que normalmente contienen información de dudosa procedencia, es la solicitud del número de teléfono móvil para completar la acción que interesa al usuario. Normalmente, si el usuario introduce el número de teléfono, además de no obtener la recompensa por la que inicialmente lo introdujo, es suscrito a servicios premium que tienen costes adicionales.
- Predisposición conocer en persona a usuarios conocidos en internet: los juegos en red, los chats e incluso las redes sociales, entre otras aplicaciones web facilitan el contacto con personas desconocidas. De este modo es posible coincidir con personas desconocidas que a través de interaccionar con los jóvenes en repetidas ocasiones pueden surgir relaciones de confianza que den lugar a encuentros en persona más allá del ámbito digital. De éste modo conoceremos la predisposición de los jóvenes a conocer en persona a una persona conocida en internet.
- Percepción humillación presencial vs online: nos permite conocer la valoración que tienen los jóvenes sobre la afección del daño que tiene insultar o vacilar a través de las TIC en comparación con los mismos hechos realizados en persona. Como podíamos ver en el análisis del ciberbullying obtenido del "Monográfico sobre el acoso escolar, ciberbullying" realizado por chaval.es, una de la características del ciberbullying es la reducción de las restricciones sociales y la dificultad para percibir el daño causado que pudiera hacer poner fin al comportamiento. Por ello, se ve necesario sensibilizar al perpetrador de la acción sobre la afección del daño del ciberbullying.

- Información previa sobre hábitos seguros y responsables en el uso de las TIC: nos permite conocer el efecto de la información que han recibido los jóvenes sobre los hábitos seguros y responsables en el uso de las TIC. De este modo se podrá analizar su influencia en la exposición a los riesgos derivados de las TIC, con respecto a aquellas personas que no han recibido información de este tipo.

Por último, en el postest se han incluido 2 preguntas adicionales con el propósito de conocer el material audiovisual eliminado y aquellas personas que han revisado la configuración de seguridad y privacidad de su red social tras la intervención.

6. Plan de análisis

Para realizar el análisis de los datos obtenidos de la aplicación de los instrumentos de evaluación utilizados, se ha requerido el uso de un programa estadístico especializado. Por las características del estudio y la funcionalidad del programa, la aplicación seleccionada es el SPSS en su versión 22, utilizando un nivel de significación de 0,05.

Los ítems planteados pretenden dar respuesta a las hipótesis que se plantean en investigación. Cada uno de los ítems se confeccionó con el objetivo de obtener información sobre la exposición de los jóvenes a cada uno de los riesgos que forman parte del estudio.

Como hemos examinado en el marco teórico, los riesgos han sido clasificados según los "derivados de las actividades de niños y niñas en términos de riesgos de contenido (en los que el niño o niña es receptor), riesgos de contacto en los que el niño o niña participa de algún modo, aunque sea involuntario y riesgos de conducta (donde el niño o niña es actor)" (Garmendia et al., 2011).

Siguiendo ésta clasificación, adaptándola a los hábitos de los jóvenes, se han definido categorías de hábitos que nos permiten agrupar los hábitos seguros y responsables de los jóvenes al utilizar las TIC que son analizados en nuestro estudio. Las categorías establecidas son las siguientes:

- Hábitos de contacto: Engloba los hábitos y decisiones de los usuarios que permiten el acceso a sus redes sociales.

- Hábitos de contenidos: hábitos relacionados con la información que se comparte a través de internet.
- Hábitos de conducta: hábitos relacionados con la conducta de los usuarios con respecto a otros usuarios y páginas web.
- Hábitos de protección: medidas proteccionistas tomadas por los usuarios para proteger sus equipos informáticos.

Cada categoría se analiza a través de los ítems especificados en la Figura 48 Asociación ítems y riesgos pretest, en la que, además, podemos apreciar la correspondencia entre los ítems que forman parte de los cuestionarios y los riesgos a los que están asociados.

- Cuestionario previo a la intervención: PRETEST

ASOCIACIÓN ENTRE ITEMS Y RIESGOS	
ITEMS	RIESGOS ASOCIADOS
Identificación y punto de partida	
1, 2, 3, 29	Se analizarán los resultados obtenidos según el género de los participantes y según el grupo (experimental/control) del que forman parte en el estudio. Además, se ha incluido el ítem 30 para analizar la influencia de la información que han recibido previamente algunos jóvenes sobre hábitos seguros y responsables, en la exposición a los riesgos.
Hábitos de contacto: control de acceso a redes sociales	
4, 8	Ciberbullying Amenazas a la privacidad Riesgos derivados del acceso de personas desconocidas a la información compartida: cibergrooming, sexting, sextorsión, etc.
Hábitos de contenidos: exposición de información personal	

Según la cercanía de las personas con las que se comparte la información	
Amigos:	
5, 9, 14	Ciberbullying Amenazas a la privacidad Sexting Sextorsión
Amigos de mis amigos	
5, 10, 15	Ciberbullying Amenazas a la privacidad Sexting Sextorsión
Conocidos en internet	
5, 11, 12, 13, 16, 21, 23, 25, 27	Ciberbullying Cibergrooming Amenazas a la privacidad Sexting Sextorsión
Según la calidad de los contenidos	
6, 7	Ciberbullying Sexting
Hábitos de conducta	
17, 22, 24, 26, 28	Amenazas técnicas, virus y fraudes. Acceso a contenidos inadecuados Vulneración de derechos de propiedad intelectual Ciberbulling
Hábitos de protección	
18, 19, 20	Amenazas técnicas y/o malware Riesgos económicos y fraudes.

	Cibergrooming Amenazas a la privacidad

Figura 48 Asociación ítems y riesgos pretest

- Cuestionario aplicado tras la intervención: POSTEST

ASOCIACIÓN ENTRE ITEMS Y RIESGOS	
ITEMS	RIESGOS ASOCIADOS
Identificación y punto de partida	
1, 2, 3, 30	Se analizarán los resultados obtenidos según el género de los participantes y según el grupo (experimental/control) del que forman parte en el estudio. Además, se ha incluido el ítem 31 para analizar la influencia de la información que han recibido previamente algunos jóvenes sobre hábitos seguros y responsables, en la exposición a los riesgos.
Hábitos de contacto: control de acceso a redes sociales	
4, 8, 9	Ciberbullying Amenazas a la privacidad Riesgos derivados del acceso de personas desconocidas a la información compartida: cibergrooming, sexting, sextorsión, etc.
Hábitos de contenidos: exposición de información personal	
Según la cercanía de las personas con las que se comparte la información	
Amigos:	
5, 10, 15	Ciberbullying Amenazas a la privacidad Sexting Sextorsión
Amigos de mis amigos	
5, 11, 16	Ciberbullying Amenazas a la privacidad

	Sexting Sextorsión
Conocidos en internet	
5, 12, 13, 14, 17, 22, 24, 26, 28	Ciberbullying Cibergrooming Amenazas a la privacidad Sexting Sextorsión
Según la calidad de los contenidos	
6, 7	Ciberbullying Sexting
Hábitos de conducta	
18, 23, 25, 27, 29	Acceso a contenidos inadecuados. Amenazas técnicas, virus y fraudes. Vulneración de derechos de propiedad intelectual Ciberbullying
Hábitos de protección	
19, 20, 21	Amenazas técnicas y/o malware Riesgos económicos y fraudes. Cibergrooming Amenazas a la privacidad

Figura 49 Asociación Infomación Postest

CAPÍTULO IV. ANÁLISIS ESTADÍSTICO Y RESULTADOS

1. Introducción

En el presente apartado se muestran los principales resultados obtenidos tras aplicar el plan de intervención diseñado con el fin paliar las consecuencias nocivas derivadas del uso de las TIC. El informe continúa con la presentación de los resultados que están organizados en fases y objetivos de la investigación.

En la fase pre-experimental, pretende dar cuenta de la equivalencia de los grupos antes de la intervención, además de conocer las necesidades y carencias, que presentan los grupos participantes en el estudio, en hábitos seguros y responsables en el uso de las TIC. Para ello, se analizarán los hábitos que tienen los jóvenes, previamente a la implementación de la intervención, del grupo experimental y del grupo de control. En el análisis de la información en la fase pre-experimental, ha sido necesario la aplicación de la prueba chi-cuadrado que permite evaluar si las variables son o no independientes entre sí, es decir si están o no relacionadas, la prueba Kolmogorov-Smirnov que nos permite conocer la distribución de los datos y la U de Mann-Whitney que es una prueba no paramétrica que nos permitirá conocer la significación en distribuciones no normales. Además, se exponen las tablas de contingencia para poder apreciar las respuestas de cada grupo.

Posteriormente, tras la aplicación del plan de intervención, en la fase postest, se obtuvieron los resultados que nos permiten analizar el efecto del programa diseñado

para el favorecimiento de los hábitos seguros y saludables de los jóvenes cuando utilizan las tecnologías de la información y de la comunicación. Esto podemos apreciarlo comparando los cambios observados en los resultados obtenidos de los cuestionarios, tras la intervención realizada.

Dentro de cada bloque que forma parte del capítulo, podemos apreciar la comparación entre los resultados obtenidos en el pretest y en el postest.

A partir de estos resúmenes informativos, se han realizado análisis bivariados de carácter exploratorio basados en la comparación cruzada entre variables.

2. Fase pre-experimental

En el desarrollo de la fase pre-experimental, se analizará la información obtenida en el pretest con el objetivo de dar respuesta a los siguientes planteamientos:

1. Por un lado, los resultados del grupo experimental nos permitirán conocer los hábitos que tienen los jóvenes al utilizar las TIC y así poder implementar una intervención adaptada a sus carencias y necesidades. Además, se analizará la exposición a los riesgos incluidos en el estudio, en el total de la muestra, para dar respuesta a la primera y segunda hipótesis que han sido planteadas en la investigación.
2. Se analizarán las condiciones de partida del grupo experimental y grupo de control para determinar si pueden ser consideradas equivalentes. No obstante, debido a que cada participante actúa de control sobre sí mismo, se minimiza el efecto que puedan tener sobre la intervención.

3. Además, se analizará la influencia del género y de la información que han recibido, algunos jóvenes, sobre hábitos seguros y responsables en el uso de las TIC en la exposición a los riesgos incluidos en el estudio.

2.1 Condiciones de partida del grupo experimental y grupo de control

Para conocer las condiciones de partida de cada uno de los grupos participantes en el estudio hemos utilizado la prueba chi-cuadrado que nos permite conocer si se obtienen diferencias significativas entre los resultados hallados en el pretest de cada uno de los grupos. Es decir, en cada variable que forma parte del estudio se aplicará la prueba chi-cuadrado para valorar si existen diferencias significativas entre los grupos respecto a la variable analizada. Además, se utilizará la prueba de Kolmogorov-Smirnov que se aplicará para contrastar la hipótesis de normalidad de la población, en cuyo caso se aplicaría un estadístico no paramétrico: U de Mann-Whitney. Por último, ha sido necesario aplicar el método de Monte Carlo para calcular p donde chi-cuadrado no es fiable y no es posible aplicar el método exacto Fisher.

Género

Tabla 1 Contingencia género

			Grupo		Total
			Colegio Control	Colegio Experimental	
Género	Hombre	Recuento	21	29	50
		% dentro de Grupo	46,7%	46,8%	46,7%
	Mujer	Recuento	24	33	57
		% dentro de Grupo	53,3%	53,2%	53,3%

Total	Recuento	45	62	107
	% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 2 Pruebas de Chi-cuadrado género

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,000[a]**	**1**	**,991**		
Corrección por continuidad	,000	1	1,000		
Razón de verosimilitudes	,000	1	,991		
Estadístico exacto de Fisher				1,000	,574
Asociación lineal por lineal	,000	1	,991		
N de casos válidos	107				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 21,03.

b. Calculado sólo para una tabla de 2x2.

No hay diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Género (Chi-cuadrado: 0,000; gl = 1; p= 0,991)

Edad

Antes de realizar la comparación entre los grupos comprobamos si la variable edad tiene o no una distribución normal.

Tabla 3 Prueba de Kolmogorov-Smirnov

		¿Cuántos años tienes?
N		107
Parámetros normales[a,b]	Media	13,69
	Desviación típica	,732
Diferencias más extremas	Absoluta	,257
	Positiva	,257
	Negativa	-,233

Z de Kolmogorov-Smirnov	**2,663**
Sig. asintót. (bilateral)	**,000**

a. La distribución de contraste es la Normal.

b. Se han calculado a partir de los datos.

Los resultados indican que la variable edad no tiene una distribución normal (ZKS: 2,663; gl=1; p<0,001).

Por tanto, para comparar la edad en el grupo experimental y el de control es necesario usar un estadístico no paramétrico: U de Mann-Whitney.

Tabla 4 Informe edad

¿Cuántos años tienes?

Grupo	Media	Mediana	Desv. típ.	N
Colegio Control	13,78	14,00	,902	45
Colegio Experimental	13,63	14,00	,579	62
Total	13,69	14,00	,732	107

Tabla 5 Rangos edad

	Grupo	N	Rango promedio	Suma de rangos
¿Cuántos años tienes?	Colegio Control	45	54,92	2471,50
	Colegio Experimental	62	53,33	3306,50
	Total	107		

Estadísticos de contraste[a]

	¿Cuántos años tienes?
U de Mann-Whitney	**1353,500**
W de Wilcoxon	3306,500
Z	**-,292**
Sig. asintót. (bilateral)	**,770**

a. Variable de agrupación: Grupo

Los resultados indican que no hay diferencias significativas entre el grupo experimental y el grupo de control respecto a la variable edad (U de M-W: 1353,5; gl=1; p=0,770).

Según estos resultados se puede decir que la composición de la muestra es homogénea respecto a género y edad.

Información previa sobre hábitos seguros y responsables en el uso de las TIC

Tabla 6 Contingencia información previa hábitos seguros y responsables

			Grupo		Total
			Colegio Control	Colegio Experimental	
Información previa hábitos seguros y responsables	No	Recuento	28	17	45
		% dentro de Grupo	62,2%	27,4%	42,1%
	Sí	Recuento	17	45	62
		% dentro de Grupo	37,8%	72,6%	57,9%
Total		Recuento	45	62	107
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 7 Pruebas de chi-cuadrado información previa hábitos seguros y responsables

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**12,960[a]**	**1**	**,000**		
Corrección por continuidad[b]	11,571	1	,001		
Razón de verosimilitudes	13,118	1	,000		
Estadístico exacto de Fisher				,000	,000
Asociación lineal por lineal	12,839	1	,000		
N de casos válidos	107				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 18,93.

b. Calculado sólo para una tabla de 2x2.

Hay diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Información previa hábitos seguros y responsables (Chi-cuadrado: 0,000; gl = 1; p< 0,001). Se aprecia que en el grupo experimental hay más jóvenes que han recibido información sobre hábitos seguros y responsables en el uso de internet. No obstante, debido a que cada sujeto actúa de control consigo mismo, se minimiza el efecto que pueda tener en la intervención

Contactos en RRSS

Tabla 8 Contingencia contactos en RRSS

			Grupo		Total
			Colegio Control	Colegio Experimental	
¿A quién aceptarías como 'amigo' en tus redes sociales?	A mis amigos	Recuento	17	26	43
		% dentro de Grupo	37,8%	41,9%	40,2%
	A mis amigos y a amigos de mis amigos	Recuento	13	19	32
		% dentro de Grupo	28,9%	30,6%	29,9%
	A mis amigos, a amigos de mis amigos y a personas que conozco en internet	Recuento	11	17	28
		% dentro de Grupo	24,4%	27,4%	26,2%
	A todo el mundo que me lo proponga	Recuento	4	0	4
		% dentro de Grupo	8,9%	0,0%	3,7%
Total		Recuento	45	62	107
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 9 Pruebas de Chi-cuadrado contactos RRSS

	Valor	gl	Sig. asintótica (bilateral)	Sig. de Monte Carlo (bilateral)		
				Sig.	Intervalo de confianza al 99%	
					Límite inferior	Límite superior
Chi-cuadrado de Pearson	5,738[a]	3	,125	,134[b]	,125	,142
Razón de verosimilitudes	7,158	3	,067	,094[b]	,086	,101
Estadístico exacto de Fisher	5,338			,145[b]	,136	,154
Asociación lineal por lineal	1,148[c]	1	,284	,324[b]	,312	,336
N de casos válidos	107					

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Contactos RRSS (Chi-cuadrado: 5,738 gl = 1; p= 0,125), donde la significación del método de Monte Carlo es 0,134.

Fotos personales en RRSS

Tabla 10 Distribución fotos personales en RRSS

	N	Parámetros normales[a,b]		Diferencias más extremas			Z de Kolmogorov-Smirnov	Sig. asintót. (bilateral)
		Media	Desviación típica	Absoluta	Positiva	Negativa		
¿Cuántas fotos, en las que apareces, tienes subidas a tus redes sociales?	107	2,20	1,299	,233	,233	-,132	**2,410**	**,000**

Podemos ver como la variable fotos personales en redes sociales no sigue distribución normal, por lo que aplicaremos el estadístico no paramétrico de U de Mann-Whitney.

Tabla 11 U de Mann-Whitney fotos personales en RRSS

	U de Mann-Whitney	W de Wilcoxon	**Z**	**Sig. asintót. (bilateral)**
¿Cuántas fotos, en las que apareces, tienes subidas a tus redes sociales?	**1172,000**	3125,000	**-1,457**	**,145**

Se observa que la variable fotos personales en redes sociales ha resultado no significativa en los resultados obtenidos en el pretest de los grupos experimental y control (p=0,145).

Percepción fotos inadecuadas en RRSS

Tabla 12 Contingencia percepción fotos inadecuadas

			Grupo		Total
			Colegio Control	Colegio Experimental	
PRETEST Alguna de las fotos, en las que apareces, que tienes compartidas en tus redes sociales, ¿podría parecerles inadecuada a tus padres si la vieran?	No	Recuento	35	58	93
		% dentro de Grupo	83,3%	96,7%	91,2%
	Sí	Recuento	7	2	9
		% dentro de Grupo	16,7%	3,3%	8,8%
Total		Recuento	42	60	102
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 13 Pruebas de chi-cuadrado percepción fotos inadecuadas

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**5,459**[a]	**1**	,019		
Corrección por continuidad[b]	3,928	1	,047		
Razón de verosimilitudes	5,496	1	,019		
Estadístico exacto de Fisher				**,031**	,024
Asociación lineal por lineal	5,406	1	,020		
N de casos válidos	102				

a. 1 casillas (25,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 3,71.

b. Calculado sólo para una tabla de 2x2.

Podemos observar que se han obtenido un 25% de casillas con frecuencias esperadas menor que 5.Sin embargo, para que chi-cuadrado se calcule correctamente tiene que haber como máximo un 20%. Hay que usar una corrección, en este caso el método exacto Fischer.

Se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable FotosInadecuadas (Chi-cuadrado: 5,46; gl = 1; p= 0,19). Por su parte, el estadístico exacto de Fisher es de 0,031. Observamos que el 83,6% de los partipantes en grupo de control y el 96,7% del grupo experimental responden 'No' a la pregunta 'Alguna de las fotos, en las que apareces, que tienes compartidas en tus redes sociales, ¿podría parecerles inadecuada a tus padres si la vieran?'.

Percepción comentario inadecuado en RRSS

Tabla 14 Contingencia percepción comentario inadecuado

			Grupo		Total
			Colegio Control	Colegio Experimental	
PRETEST ¿Alguno de los comentarios, que tienes en tus redes sociales, podría parecerles inadecuado a tus padres si lo vieran?	No	Recuento	27	51	78
		% dentro de Grupo	64,3%	85,0%	76,5%
	Sí	Recuento	15	9	24
		% dentro de Grupo	35,7%	15,0%	23,5%
Total		Recuento	42	60	102
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 15 Pruebas de chi-cuadrado percepción comentario inadecuado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**5,892[a]**	**1**	**,015**		
Corrección por continuidad[b]	4,797	1	,029		
Razón de verosimilitudes	5,829	1	,016		
Estadístico exacto de Fisher				,019	,015
Asociación lineal por lineal	5,834	1	,016		
N de casos válidos	102				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 9,88.

b. Calculado sólo para una tabla de 2x2.

Se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable ComentariosInadecuados (Chi-cuadrado: 5,89; gl = 1; p= 0,15). Observamos que el 64,3% de los partipantes en grupo de control y el 85% del grupo experimental responden 'No' a la pregunta 'Alguno de los comentarios, que tienes en tus redes sociales, podría parecerles inadecuado a tus padres si lo vieran?'.

Configuración seguridad y privacidad en RRSS

Tabla 16 Contingencia configurar privacidad

			Grupo		Total
			Colegio Control	Colegio Experimental	
¿Consideras necesario configurar tú mismo/a la seguridad y privacidad de tus redes sociales?	No	Recuento	21	35	56
		% dentro de Grupo	47,7%	58,3%	53,8%
	Sí	Recuento	23	25	48
		% dentro de Grupo	52,3%	41,7%	46,2%
Total		Recuento	44	60	104
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 17 Pruebas de chi-cuadrado configurar privacidad.

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**1,149[a]**	**1**	**,284**		
Corrección por continuidad[b]	,762	1	,383		
Razón de verosimilitudes	1,149	1	,284		
Estadístico exacto de Fisher				,323	,191
Asociación lineal por lineal	1,138	1	,286		
N de casos válidos	104				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 20,31.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Configurar Privacidad (Chi-cuadrado: 1,149 gl = 1; p= 0,284).

Predisposición a compartir fotos o vídeos personales con amigos

Tabla 18 Contingencia compartir fotos o vídeos con amigos

			Grupo		Total
			Colegio Control	Colegio Experimental	
De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con mis amigos]	No	Recuento	4	4	8
		% dentro de Grupo	8,9%	6,5%	7,5%
	Sí	Recuento	41	58	99
		% dentro de Grupo	91,1%	93,5%	92,5%
Total		Recuento	45	62	107
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 19 Pruebas de chi-cuadrado compartir fotos o vídeos con amigos

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,224[a]**	1	,636		
Corrección por continuidad[b]	,010	1	,920		
Razón de verosimilitudes	,221	1	,638		
Estadístico exacto de Fisher				**,718**	,453
Asociación lineal por lineal	,222	1	,638		
N de casos válidos	107				

a. 2 casillas (50,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 3,36.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Compartir con Amigos (Chi-cuadrado: 0,224; gl = 1; p= ,636). En éste caso, debido a que se obtiene que el 50% tienen una frecuencia esperada inferior a 5, observamos el estadístico exacto de Fischer para conocer la significación. Dado que el resultado obtenido es 0,718 queda demostrado que no se hallan diferencias significativas entre las variables analizadas.

Predisposición a compartir fotos o vídeos personales con amigos de mis amigos

Tabla 20 Contingencia compartir fotos o vídeos con amigos de mis amigos

			Grupo		Total
			Colegio Control	Colegio Experimental	
De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con amigos de mis amigos]	No	Recuento	19	27	46
		% dentro de Grupo	42,2%	43,5%	43,0%
	Sí	Recuento	26	35	61
		% dentro de Grupo	57,8%	56,5%	57,0%
Total		Recuento	45	62	107

	% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 21 Pruebas de chi-cuadrado compartir fotos o vídeos con amigos de mis amigos

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,019[a]**	**1**	**,891**		
Corrección por continuidad[b]	,000	1	1,000		
Razón de verosimilitudes	,019	1	,891		
Estadístico exacto de Fisher				1,000	,525
Asociación lineal por lineal	,019	1	,892		
N de casos válidos	107				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 19,35.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Compartir con amigos de mis amigos (Chi-cuadrado: 0,019 gl = 1; p= 0,891)

Predisposición a compartir fotos o vídeos con conocidos en internet

Tabla 22 Contingencia compartir fotos o vídeos con conocidos en internet

			Grupo		Total
			Colegio Control	Colegio Experimental	
De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con personas que he conocido en internet]	No	Recuento	30	46	76
		% dentro de Grupo	66,7%	74,2%	71,0%
	Sí	Recuento	15	16	31
		% dentro de Grupo	33,3%	25,8%	29,0%
Total		Recuento	45	62	107
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 23 Pruebas de chi-cuadrado compartir fotos o vídeos con conocidos en internet

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,718[a]**	**1**	**,397**		
Corrección por continuidad	,399	1	,528		
Razón de verosimilitudes	,714	1	,398		
Estadístico exacto de Fisher				,518	,263
Asociación lineal por lineal	,711	1	,399		
N de casos válidos	107				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 13,04.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Compartir con conocidos en internet (Chi-cuadrado: 0,718 gl = 1; p= 0,397)

Predisposición a compartir información con conocidos en internet (E-mail, nº de teléfono)

- *Predisposición a compartir e-mail con personas conocidas en internet*

Tabla 24 Predisposición a compartir e-mail con personas conocidas en internet

			Grupo		Total
			Colegio Control	Colegio Experimental	
Email	No	Recuento	37	58	95
		% dentro de Grupo	82,2%	93,5%	88,8%
	Sí	Recuento	8	4	12
		% dentro de Grupo	17,8%	6,5%	11,2%
Total		Recuento	45	62	107
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 25 Prueba chi-cuadrado predisposición a compartir e-mail con personas conocidas en internet

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	3,359[a]	1	,067		
Corrección por continuidad[b]	2,318	1	,128		
Razón de verosimilitudes	3,327	1	,068		
Estadístico exacto de Fisher				,118	,065
Asociación lineal por lineal	3,328	1	,068		
N de casos válidos	107				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 5,05.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Compartir e-mail desconocidos (Chi-cuadrado: 3,359; gl = 1; p= 0,067)

- *Predisposición a Compartir número de teléfono con personas conocidas en internet*

Tabla 26 Contingencia predisposición a compartir teléfono desconocidos

			Grupo		Total
			Colegio Control	Colegio Experimental	
PRETEST Número de teléfono	No	Recuento	36	59	95
		% dentro de Grupo	80,0%	95,2%	88,8%
	Sí	Recuento	9	3	12
		% dentro de Grupo	20,0%	4,8%	11,2%
Total		Recuento	45	62	107
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 27 Prueba chi-cuadrado predisposición a compartir teléfono desconocidos

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	6,019[a]	1	,014		
Corrección por continuidad[b]	4,593	1	,032		
Razón de verosimilitudes	6,051	1	,014		
Estadístico exacto de Fisher				,026	,016
Asociación lineal por lineal	5,963	1	,015		
N de casos válidos	107				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 5,05.

b. Calculado sólo para una tabla de 2x2.

Se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Compartir teléfono desconocidos (Chi-cuadrado: 6,019; gl = 1; p= 0,14).

Predisposición uso de la webcam con amigos

Tabla 28 Predisposición uso de la webcam con amigos

Grupo		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Colegio Control	No	23	51,1	51,1	51,1
	Sí	22	48,9	48,9	100,0
	Total	45	100,0	100,0	
Colegio Experimental	No	29	46,8	46,8	46,8
	Sí	33	53,2	53,2	100,0
	Total	62	100,0	100,0	

Tabla 29 Contingencia uso de webcam con amigos

			Grupo		Total
			Colegio Control	Colegio Experimental	
PRETEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con mis amigos]	No	Recuento	23	29	52
		% dentro de Grupo	51,1%	46,8%	48,6%
	Sí	Recuento	22	33	55
		% dentro de Grupo	48,9%	53,2%	51,4%
Total		Recuento	45	62	107
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 30 Pruebas de chi-cuadrado uso de webcam con amigos

	Valor	Gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,196[a]**	**1**	**,658**		
Corrección por continuidad	,061	1	,805		
Razón de verosimilitudes	,196	1	,658		
Estadístico exacto de Fisher				,698	,402
Asociación lineal por lineal	,194	1	,659		
N de casos válidos	107				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 21,87.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable webcam con amigos (Chi-cuadrado: 0,196 gl = 1; p= 0,658)

Predisposición uso de la webcam con amigos de mis amigos

Tabla 31 Contingencia uso de webcam con amigos de mis amigos

			Grupo		Total
			Colegio Control	Colegio Experimental	
PRETEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con amigos de mis amigos]	No	Recuento	39	56	95
		% dentro de Grupo	86,7%	90,3%	88,8%
	Sí	Recuento	6	6	12
		% dentro de Grupo	13,3%	9,7%	11,2%
Total		Recuento	45	62	107
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 32 Pruebas de chi-cuadrado uso de webcam con amigos de mis amigos

	Valor	Gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,350[a]**	**1**	**,554**		
Corrección por continuidad[b]	,079	1	,778		
Razón de verosimilitudes	,346	1	,556		
Estadístico exacto de Fisher				,554	,385
Asociación lineal por lineal	,347	1	,556		
N de casos válidos	107				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 5,05.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Webcam con amigos de mis amigos (Chi-cuadrado=0,350; gl = 1; p= 0,554).

Predisposición uso de la webcam con conocidos en internet

Tabla 33 Contingencia uso de la webcam con conocidos en internet

			Grupo		Total
			Colegio Control	Colegio Experimental	
PRETEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Conocidos en internet]	No	Recuento	45	58	103
		% dentro de Grupo	100,0%	93,5%	96,3%
	Sí	Recuento	0	4	4
		% dentro de Grupo	0,0%	6,5%	3,7%
Total		Recuento	45	62	107
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 34 Pruebas de chi-cuadrado uso de webcam con conocidos en internet

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**3,016[a]**	**1**	,082		
Corrección por continuidad[b]	1,490	1	,222		
Razón de verosimilitudes	4,478	1	,034		
Estadístico exacto de Fisher				**,137**	,108
Asociación lineal por lineal	2,988	1	,084		
N de casos válidos	107				

a. 2 casillas (50,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 1,68.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Webcam con conocidos en internet (Chi-cuadrado=3,016; gl = 1; p= 0,082). Se obtiene, además, 50% de las casillas con una frecuencia esperada inferior a 5, por lo que se recurre al estadístico exacto de Fisher que corrobora que no se hallan diferencias significativas al obtener 0,137.

Humillación a terceros en RRSS

Tabla 35 Contingencia burlarse de una foto o comentario

			Grupo		Total
			Colegio Control	Colegio Experimental	
PRETEST ¿Alguna vez te has burlado de un comentario o foto en una red social?	No	Recuento	18	37	55
		% dentro de Grupo	42,9%	59,7%	52,9%
	Sí	Recuento	24	25	49
		% dentro de Grupo	57,1%	40,3%	47,1%
Total		Recuento	42	62	104
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 36 Pruebas de chi-cuadrado de contingencia burlarse de una foto o comentario

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**2,843[a]**	**1**	**,092**		
Corrección por continuidad[b]	2,208	1	,137		
Razón de verosimilitudes	2,851	1	,091		
Estadístico exacto de Fisher				,111	,069
Asociación lineal por lineal	2,816	1	,093		
N de casos válidos	104				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 19,79.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable burlarse de una foto o comentario (Chi-cuadrado: 2,843; gl = 1; p=0,92).

Uso de Software de protección en el ordenador

Tabla 37 Contingencia uso software de protección en el ordenador

			Grupo		Total
			Colegio Control	Colegio Experimental	
PRETEST ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu ordenador de casa?	No	Recuento	11	3	14
		% dentro de Grupo	27,5%	4,9%	13,9%
	Sí	Recuento	29	58	87
		% dentro de Grupo	72,5%	95,1%	86,1%
Total		Recuento	40	61	101
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 38 Pruebas de chi-cuadrado uso software de protección en el ordenador

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**10,318[a]**	**1**	**,001**		
Corrección por continuidad[b]	8,513	1	,004		
Razón de verosimilitudes	10,316	1	,001		
Estadístico exacto de Fisher				,002	,002
Asociación lineal por lineal	10,216	1	,001		
N de casos válidos	101				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 5,54.

b. Calculado sólo para una tabla de 2x2.

Se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Software de protección en el ordenador (Chi-cuadrado: 10,318; gl = 1; p= 0,001). Los jóvenes que tienen instalado software de protección en el ordenador de casa asciende al 72,5% en el grupo de control y al 95,1% en el grupo experimental.

Uso de software de protección en el Smartphone

Tabla 39 Contingencia uso software de protección en el Smartphone

			Grupo		Total
			Colegio Control	Colegio Experimental	
PRETEST ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu Smartphone?	No	Recuento	17	20	37
		% dentro de Grupo	48,6%	35,1%	40,2%
	Sí	Recuento	18	37	55
		% dentro de Grupo	51,4%	64,9%	59,8%
Total		Recuento	35	57	92
		% dentro de Grupo	100,0%	100,0%	100,0%

Tabla 40 Pruebas de chi-cuadrado uso software de protección en el Smartphone

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**1,640[a]**	**1**	**,200**		
Corrección por continuidad	1,127	1	,288		
Razón de verosimilitudes	1,632	1	,201		
Estadístico exacto de Fisher				,274	,144
Asociación lineal por lineal	1,622	1	,203		
N de casos válidos	92				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 14,08.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Software de protección en el Smartphone (Chi-cuadrado: 1,640; gl =1; p= 0,200). Los jóvenes que disponen de software de protección en su Smartphone es del 51,4% en el grupo del control y de un 64,9% en el grupo experimental.

A continuación, se analizarán las variables que han utilizado una escala de 5 opciones de respuesta de escala Likert. No obstante, antes de realizar las pruebas de comparación, se verifica si las variables cumplen el supuesto de normalidad.

Tabla 41 Prueba de Kolmogorov-Smirnov escala Likert

	N	Parámetros normales[a,b]		Diferencias más extremas			Z de Kolmogorov-Smirnov	Sig. asintót. (bilateral)
		Media	Desviación típica	Absoluta	Positiva	Negativa		
Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	107	4,51	,945	,425	,304	-,425	**4,400**	**,000**
Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	107	1,75	1,166	,365	,365	-,261	**3,780**	**,000**
Sólo entro en páginas web recomendadas para mi edad	107	3,11	1,494	,158	,146	-,158	**1,639**	**,009**
Los chats públicos son páginas seguras donde nadie puede hacerme nada	107	2,35	1,282	,199	,199	-,147	**2,057**	**,000**
No pasa nada por descargar música o aplicaciones “pirateadas”	107	3,04	1,281	,185	,185	-,171	**1,909**	**,001**
Si conozco a alguien simpático/a jugando en red, le agregaría como ‘amigo/a’ en mi red social	107	2,36	1,319	,212	,212	-,152	**2,196**	**,000**
Si una página web me pide el número de teléfono, se lo doy	107	1,72	1,139	,372	,372	-,264	**3,845**	**,000**

Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	107	1,68	1,146	,397	,397	-,276	**4,108**	**,000**
Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	107	1,93	1,261	,331	,331	-,229	**3,429**	**,000**

a. La distribución de contraste es la Normal.

b. Se han calculado a partir de los datos.

Podemos observar que el nivel de significación de la prueba Kolmogorov-Smirnov es menor que 0,05 en todas las variables por lo que no siguen una distribución normal. Por tanto, se deben usar estadísticos no paramétricos. Usamos U de Mann-Whitney para verificar si hay diferencias significativas en el pretest entre el grupo experimental y el de control.

Tabla 42 Informe descriptivo escala Likert

	Grupo										
	Colegio Control				Colegio Experimental				Total		
	N	Media	Mediana	Desv. típ.	N	Media	Mediana	Desv. típ.	Media	Mediana	Desv. típ.
Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	45	4,36	5,00	1,151	62	4,63	5,00	,752	4,51	5,00	,945
Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	45	1,93	1,00	1,388	62	1,61	1,00	,964	1,75	1,00	1,166
Sólo entro en páginas web recomendadas para mi edad	45	2,76	3,00	1,479	62	3,37	3,50	1,462	3,11	3,00	1,494

Los chats públicos son páginas seguras donde nadie puede hacerme nada	45	2,16	2,00	1,278	62	2,48	2,00	1,277	2,35	2,00	1,282
No pasa nada por descargar música o aplicaciones "pirateadas"	45	3,02	3,00	1,357	62	3,05	3,00	1,234	3,04	3,00	1,281
Si conozco a alguien simpático/a jugando en red, le agregaría como 'amigo/a' en mi red social	45	2,44	2,00	1,486	62	2,29	2,00	1,193	2,36	2,00	1,319
Si una página web me pide el número de teléfono, se lo doy	45	1,73	1,00	1,095	62	1,71	1,00	1,179	1,72	1,00	1,139
Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	45	1,78	1,00	1,295	62	1,61	1,00	1,030	1,68	1,00	1,146
Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	45	2,18	2,00	1,353	62	1,76	1,00	1,169	1,93	1,00	1,261

Estas son las pruebas de comparación de U de Mann-Whitney para los grupos experimental y de control.

Tabla 43 Estadísticos de contraste escala Likert

	U de Mann-Whitney	W de Wilcoxon	**Z**	**Sig. asintót. (bilateral)**
Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	**1270,000**	2305,000	**-1,010**	**,312**
Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	**1278,000**	3231,000	**-,853**	**,394**
Sólo entro en páginas web recomendadas para mi edad	**1069,000**	2104,000	**-2,108**	**,035**

Los chats públicos son páginas seguras donde nadie puede hacerme nada	**1173,000**	2208,000	**-1,454**	**,146**
No pasa nada por descargar música o aplicaciones "pirateadas"	**1379,000**	2414,000	**-,104**	**,917**
Si conozco a alguien simpático/a jugando en red, le agregaría como 'amigo/a' en mi red social	**1358,000**	3311,000	**-,242**	**,809**
Si una página web me pide el número de teléfono, se lo doy	**1358,000**	3311,000	**-,272**	**,786**
Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	**1348,500**	3301,500	**-,353**	**,724**
Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	**1144,000**	3097,000	**-1,754**	**,079**

a. Variable de agrupación: Grupo

No hay diferencias significativas entre el grupo experimental y el de control respecto a las variables que utilizan escala Likert, excepto para la variable 'sólo entro en páginas web recomendadas para mi edad' donde el grupo experimental tiene un promedio más alto en esta pregunta con una mediana de 3 y el grupo de control obtiene una mediana de 3,5.

Podemos concluir que la línea base o punto de partida es similar en ambos grupos, aunque como hemos podido apreciar existen diferencias entre el grupo experimental y control en las variables: 'Solo entro en páginas web recomendadas para mi edad', 'Software de protección en el ordenador', 'Comentarios inadecuados', 'Fotos inadecuadas' y en los jóvenes que han recibido información sobre hábitos seguros en el

uso de las TIC que podrían explicar diferencias significativas obtenidas en la exposición a los riesgos mencionados. No obstante, analizaremos la eficacia de la intervención tomando como control a cada sujeto, por lo que se minimiza su efecto en la intervención.

2.1.1. Análisis de la influencia de la variable "género"

A continuación, testearemos la influencia de la variable género en las variables incluidas en el estudiado.

Además, usamos chi-cuadrado para contrastar si existen diferencias entre hombres y mujeres respecto a sus respuestas en el pretest. Usamos el pretest para ver el efecto 'puro' del género, sin haber pasado por la intervención por lo que se incluye al total de la muestra.

Contactos en RRSS

Tabla 44 Contingencia contactos en RRSS

			Género		Total
			Hombre	Mujer	
¿A quién aceptarías como 'amigo' en tus redes sociales?	A mis amigos	Recuento	40	53	93
		% dentro de Género	88,9%	93,0%	91,2%
	A mis amigos y a amigos de mis amigos	Recuento	5	4	9
		% dentro de Género	11,1%	7,0%	8,8%
	A mis amigos, a amigos de mis amigos y a personas que conozco en internet	Recuento	25	18	43
		% dentro de Género	50,0%	31,6%	40,2%
	A todo el mundo que me lo proponga	Recuento	14	18	32
		% dentro de Género	28,0%	31,6%	29,9%
Total		Recuento	45	10	18
		% dentro de Género	100,0%	20,0%	31,6%

Tabla 45 Prueba chi-cuadrado contacto en RRSS

Grupo		Valor	gl	Sig. asintótica (bilateral)	Sig. de Monte Carlo (bilateral)		
					Sig.	Intervalo de confianza al 99%	
						Límite inferior	Límite superior
Total	Chi-cuadrado de Pearson	4,487[a]	3	,213	,228	,217	,239
	Razón de verosimilitudes	4,552	3	,208	,260	,249	,271
	Estadístico exacto de Fisher	4,373			,235	,224	,246
	Asociación lineal por lineal	4,353[c]	1	,037	,040	,035	,045
	N de casos válidos	107					

0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 7,95.

El estadístico tipificado es 2,398.

No se aprecian diferencias significativas respecto a los contactos que tienen los participantes en las RRSS según su género (Chi-cuadrado: 4,487; gl = 3; p= 0,213).

Fotos personales en RRSS

Tabla 46 Informe fotos compartidas en RRSS

	Género								
	Hombre			Mujer			Total		
	Media	Mediana	Desv. típ.	Media	Mediana	Desv. típ.	Media	Mediana	Desv. típ.
¿Cuántas fotos, en las que apareces, tienes subidas a tus redes sociales?	1,80	1,50	1,278	2,54	2,00	1,226	2,20	2,00	1,299

Tabla 47 Prueba U de Mann-Whitney fotos personales en RRSS

	U de Mann-Whitney	W de Wilcoxon	**Z**	**Sig. asintót. (bilateral)**
¿Cuántas fotos, en las que apareces, tienes subidas a tus redes sociales?	**922,000**	2197,000	**-3,252**	**,001**

Se hallan diferencias significativas entre hombres y mujeres respecto al número de fotos que los jóvenes tienen subidas a sus redes sociales (U de M-W: 922: Z= -3,252; p=0,001). Sólo se hallan diferencias significativas entre hombres y mujeres respecto al número de fotos que los jóvenes tienen subidas a sus redes sociales (U de M-W: 922: Z= -3,252; p=0,001), siendo las mujeres quienes disponen de más información de este tipo en sus redes sociales. La mediana que se obtiene en el caso de los hombres es de 1,5 y de 2 en el caso de mujeres.

Percepción fotos inadecuadas en RRSS

Tabla 48 Contingencia percepción fotos inadecuadas en RRSS

			Género		Total
			Hombre	Mujer	
Alguna de las fotos, en las que apareces, que tienes compartidas en tus redes sociales, ¿podría parecerles inadecuada a tus padres si la vieran?	No	Recuento	40	53	93
		% dentro de Género	88,9%	93,0%	91,2%
	Sí	Recuento	5	4	9
		% dentro de Género	11,1%	7,0%	8,8%
Total		Recuento	45	57	102
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 49 Pruebas de chi-cuadrado percepción fotos inadecuadas en RRSS

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,524**[a]	1	,469		
Corrección por continuidad[b]	,139	1	,710		
Razón de verosimilitudes	,519	1	,471		
Estadístico exacto de Fisher				**,503**	,352
Asociación lineal por lineal	,519	1	,471		
N de casos válidos	102				

a. **1 casillas (25,0%)** tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 3,97.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Fotos Inadecuadas (Chi-cuadrado: 0,524; gl = 1; p= 0,469). En éste caso el 25% de las casillas tienen una frecuencia esperada inferior a 5, por lo que observamos el estadístico exacto de Fisher que confirma la inexistencia de diferencias significativas al obtener un 0,503.

Percepción comentarios inadecuados en RRSS

Tabla 50 Contingencia percepción comentarios inadecuados en RRSS

			Género		Total
			Hombre	Mujer	
¿Alguno de los comentarios, que tienes en tus redes sociales, podría parecerles inadecuado a tus padres si lo vieran?	No	Recuento	34	44	78
		% dentro de Género	75,6%	77,2%	76,5%
	Sí	Recuento	11	13	24
		% dentro de Género	24,4%	22,8%	23,5%
Total		Recuento	45	57	102
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 51 Pruebas de chi-cuadrado percepción comentarios inadecuados en RRSS

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,037[a]**	**1**	**,847**		
Corrección por continuidad[b]	,000	1	1,000		
Razón de verosimilitudes	,037	1	,847		
Estadístico exacto de Fisher				1,000	,515
Asociación lineal por lineal	,037	1	,847		
N de casos válidos	102				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 10,59.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable comentario inadecuados (Chi-cuadrado: 0,037; gl =1; p= 0,847).

Configuración seguridad y privacidad en RRSS

Tabla 52 Contingencia configuración seguridad y privacidad en RRSS

			Género		Total
			Hombre	Mujer	
¿Consideras necesario configurar tú mismo/a la seguridad y privacidad de tus redes sociales?	No	Recuento	28	28	56
		% dentro de Género	58,3%	50,0%	53,8%
	Sí	Recuento	20	28	48
		% dentro de Género	41,7%	50,0%	46,2%
Total		Recuento	48	56	104
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 53 Pruebas de chi-cuadrado configuración seguridad y privacidad en RRSS

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,722[a]**	**1**	**,395**		
Corrección por continuidad[b]	,426	1	,514		
Razón de verosimilitudes	,724	1	,395		
Estadístico exacto de Fisher				,435	,257
Asociación lineal por lineal	,715	1	,398		
N de casos válidos	104				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 22,15.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable configurar privacidad (Chi-cuadrado: 0,722; gl = 1; p= 0,395).

Predisposición compartir fotos o vídeos personales con amigos

Tabla 54 Contingencia predisposición compartir fotos o vídeos personales con amigos

			Género		Total
			Hombre	Mujer	
De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con mis amigos]	No	Recuento	3	5	8
		% dentro de Género	6,0%	8,8%	7,5%
	Sí	Recuento	47	52	99
		% dentro de Género	94,0%	91,2%	92,5%
Total		Recuento	50	57	107
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 55 Pruebas de chi-cuadrado predisposición compartir fotos o vídeos personales con amigos

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,296[a]**	**1**	**,586**		
Corrección por continuidad[b]	,031	1	,861		
Razón de verosimilitudes	,300	1	,584		
Estadístico exacto de Fisher				,721	,434
Asociación lineal por lineal	,293	1	,588		
N de casos válidos	107				

a. **2 casillas (50,0%)** tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 3,74.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable compartir con amigos (Chi-cuadrado: 0,296; gl = 1; p=0,586).

Predisposición compartir fotos o vídeos con amigos de mis amigos

Tabla 56 Contingencia predisposición compartir fotos o vídeos con amigos de mis amigos

			Género		Total
			Hombre	Mujer	
De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con amigos de mis amigos]	No	Recuento	25	21	46
		% dentro de Género	50,0%	36,8%	43,0%
	Sí	Recuento	25	36	61
		% dentro de Género	50,0%	63,2%	57,0%
Total		Recuento	50	57	107
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 57 Pruebas de chi-cuadrado predisposición compartir fotos o vídeos con amigos de mis amigos

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**1,882[a]**	**1**	**,170**		
Corrección por continuidad[b]	1,383	1	,240		
Razón de verosimilitudes	1,884	1	,170		
Estadístico exacto de Fisher				,178	,120
Asociación lineal por lineal	1,864	1	,172		
N de casos válidos	107				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 21,50.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable compartir con amigos de mis amigos (Chi-cuadrado: 1,882; gl = 1; p= 0,170).

Predisposición a compartir fotos o vídeos personales con conocidos en internet

Tabla 58 Contingencia compartir fotos/vídeos con conocidos en internet-género

			Género		Total
			Hombre	Mujer	
De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con personas que he conocido en internet]	No	Recuento	35	41	76
		% dentro de Género	70,0%	71,9%	71,0%
	Sí	Recuento	15	16	31
		% dentro de Género	30,0%	28,1%	29,0%
Total		Recuento	50	57	107
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 59 Pruebas de chi-cuadrado compartir fotos/vídeos con conocidos en internet-género

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,048[a]**	**1**	**,826**		
Corrección por continuidad[b]	,000	1	,995		
Razón de verosimilitudes	,048	1	,826		
Estadístico exacto de Fisher				,834	,497
Asociación lineal por lineal	,048	1	,827		
N de casos válidos	107				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 14,49.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable compartir con personas conocidas en internet (Chi-cuadrado: 0,048; gl = 1; p= 0,826).

Predisposición a compartir información con desconocidos

Tabla 60 Contingencia predisposición a compartir e-mail con desconocidos

			Género		Total
			Hombre	Mujer	
¿Qué tipo de información compartirías con personas conocidas en internet? [e-mail]	No	Recuento	42	53	95
		% dentro de Género	84,0%	93,0%	88,8%
	Sí	Recuento	8	4	12
		% dentro de Género	16,0%	7,0%	11,2%
Total		Recuento	50	50	57
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 61 Prueba Chi-cuadrado predisposición a compartir e-mail con desconocidos

	Valor	Gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**2,158a**	1	**,142**		
Corrección por continuidad[b]	1,350	1	,245		
Razón de verosimilitudes	2,177	1	,140		
Estadístico exacto de Fisher				,219	,123
Asociación lineal por lineal	2,138	1	,144		
N de casos válidos	107				

a. 2 casillas (50,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 1,87

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable compartir e-mail con desconocidos (Chi-cuadrado: 2,158; gl = 1; p= 0,142). En éste caso, debido a que se obtiene que el 50% tienen una frecuencias esperada inferior a 5, observamos el estadístico exacto de Fischer para conocer la significación, que obtiene 0,219 quedando demostrado que no se hallan diferencias significativas.

Tabla 62 Contingencia predisposición a compartir nº de teléfono con desconocidos

			Género		Total
			Hombre	Mujer	
¿Qué tipo de información compartirías con personas conocidas en internet? [teléfono]	No	Recuento	42	53	95
		% dentro de Género	84,0%	93,0%	88,8%
	Sí	Recuento	8	4	12
		% dentro de Género	16,0%	7,0%	11,2%
Total		Recuento	50	50	57
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 63 Prueba chi-cuadrado predisposición a compartir nº de teléfono con desconocidos

	Valor	Gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	2,158a	1	,142		
Corrección por continuidad[b]	1,350	1	,245		
Razón de verosimilitudes	2,177	1	,140		
Estadístico exacto de Fisher				,219	,123
Asociación lineal por lineal	2,138	1	,144		
N de casos válidos	107				

a. 2 casillas (50,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 1,40.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable compartir teléfono con desconocidos (Chi-cuadrado: 2,158; gl = 1; p= 0,142). En éste caso, debido a que se obtiene que el 50% tienen una frecuencia esperada inferior a 5, observamos el estadístico exacto de Fischer

Predisposición uso de webcam con amigos

Tabla 64 Contingencia predisposición uso de webcam con amigos

			Género		Total
			Hombre	Mujer	
De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con mis amigos]	No	Recuento	27	25	52
		% dentro de Género	54,0%	43,9%	48,6%
	Sí	Recuento	23	32	55
		% dentro de Género	46,0%	56,1%	51,4%
Total		Recuento	50	57	107
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 65 Pruebas de chi-cuadrado predisposición uso de webcam con amigos

	Valor	Gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**1,096[a]**	**1**	**,295**		
Corrección por continuidad[b]	,728	1	,394		
Razón de verosimilitudes	1,098	1	,295		
Estadístico exacto de Fisher				,336	,197
Asociación lineal por lineal	1,086	1	,297		
N de casos válidos	107				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 24,30.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable webcam con amigos (Chi-cuadrado: 1,096; gl = 1; p= 0,295).

Predisposición uso de la webcam con amigos de amigos

Tabla 66 Contingencia predisposición uso de la webcam con amigos de amigos

			Género		Total
			Hombre	Mujer	
De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con amigos de mis amigos]	No	Recuento	46	49	95
		% dentro de Género	92,0%	86,0%	88,8%
	Sí	Recuento	4	8	12
		% dentro de Género	8,0%	14,0%	11,2%
Total		Recuento	50	57	107
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 67 Pruebas de chi-cuadrado predisposición uso de la webcam con amigos de amigos

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,974[a]**	**1**	**,324**		
Corrección por continuidad[b]	,462	1	,496		
Razón de verosimilitudes	,996	1	,318		
Estadístico exacto de Fisher				,373	,250
Asociación lineal por lineal	,965	1	,326		
N de casos válidos	107				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 5,61.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable webcam con amigos de mis amigos (Chi-cuadrado: 0,974; gl = 1; p= 0,324).

Predisposición uso de la webcam con conocidos en internet

Tabla 68 Contingencia predisposición uso de la webcam con conocidos en internet

			Género		Total
			Hombre	Mujer	
De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Conocidos en internet]	No	Recuento	49	54	103
		% dentro de Género	98,0%	94,7%	96,3%
	Sí	Recuento	1	3	4
		% dentro de Género	2,0%	5,3%	3,7%
Total		Recuento	50	57	107
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 69 Pruebas de chi-cuadrado predisposición uso de la webcam con conocidos en internet

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,788[a]**	**1**	,375		
Corrección por continuidad[b]	,142	1	,706		
Razón de verosimilitudes	,831	1	,362		
Estadístico exacto de Fisher				**,621**	,360
Asociación lineal por lineal	,781	1	,377		
N de casos válidos	107				

a. **2 casillas (50,0%)** tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 1,87.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable webcam conocidos en internet (Chi-cuadrado: 0,778; gl = 1; p= 0,375). En éste caso, debido a que se obtiene que el 50% tienen una frecuencias esperada inferior a 5, observamos el estadístico exacto de Fischer para conocer la significación, que obtiene 0,621 quedando demostrado que no se hallan diferencias significativas.

Humillación a terceros en RRSS

Tabla 70 Contingencia humillación a terceros en RRSS

			Género		Total
			Hombre	Mujer	
¿Alguna vez te has burlado de un comentario o foto en una red social?	No	Recuento	22	33	55
		% dentro de Género	46,8%	57,9%	52,9%
	Sí	Recuento	25	24	49
		% dentro de Género	53,2%	42,1%	47,1%
Total		Recuento	47	57	104
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 71 Pruebas de chi-cuadrado humillación a terceros en RRSS

	Valor	Gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**1,271[a]**	**1**	**,260**		
Corrección por continuidad[b]	,865	1	,352		
Razón de verosimilitudes	1,272	1	,259		
Estadístico exacto de Fisher				,325	,176
Asociación lineal por lineal	1,258	1	,262		
N de casos válidos	104				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 22,14.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable burlarse de un comentario o una foto (Chi-cuadrado: 1,271; gl = 1; p= 0,260).

Uso de software de protección en el ordenador

Tabla 72 Contingencia uso de software de protección en el ordenador

			Género		Total
			Hombre	Mujer	
¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu ordenador de casa?	No	Recuento	8	6	14
		% dentro de Género	17,4%	10,9%	13,9%
	Sí	Recuento	38	49	87
		% dentro de Género	82,6%	89,1%	86,1%
Total		Recuento	46	55	101
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 73 Pruebas de chi-cuadrado uso de software de protección en el ordenador

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,882[a]**	**1**	**,348**		
Corrección por continuidad[b]	,422	1	,516		
Razón de verosimilitudes	,878	1	,349		
Estadístico exacto de Fisher				,396	,257
Asociación lineal por lineal	,873	1	,350		

N de casos válidos	101

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 6,38.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable antivirus en el ordenador (Chi-cuadrado: 0,882; gl = 1; p= 0,348).

Uso de software de protección en el smartphone

Tabla 74 Contingencia uso de software de protección en el smartphone

			Género		Total
			Hombre	Mujer	
¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu Smartphone?	No	Recuento	18	19	37
		% dentro de Género	40,9%	39,6%	40,2%
	Sí	Recuento	26	29	55
		% dentro de Género	59,1%	60,4%	59,8%
Total		Recuento	44	48	92
		% dentro de Género	100,0%	100,0%	100,0%

Tabla 75 Pruebas de chi-cuadrado Uso de software de protección en el smartphone

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,017[a]**	**1**	**,897**		
Corrección por continuidad[b]	,000	1	1,000		
Razón de verosimilitudes	,017	1	,897		
Estadístico exacto de Fisher				1,000	,533

Asociación lineal por lineal	,017	1	,897
N de casos válidos	92		

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 17,70.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre el grupo de control y el grupo experimental respecto a la variable Software de protección en el Smartphone (Chi-cuadrado: 0,017; gl = 1; p= 0,897).

Hemos podido comprobar que en la muestra no se hallaron diferencias por género en ninguna de las variables analizadas de hábitos seguros y responsables en el uso de las TIC.

Variables que utilizan la escala Likert

A continuación, debido que el resto de variables no utilizan una distribución normal, tal y como hemos comprobado anteriormente, es necesario utilizar la prueba U de Mann-Whitney.

Tabla 76 Estadísticos descriptivos escala Likert

	Género								
	Hombre			Mujer			Total		
	Media	Mediana	Desv. típ.	Media	Mediana	Desv. típ.	Media	Mediana	Desv. típ.
Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	4,50	5,00	1,074	4,53	5,00	,826	4,51	5,00	,945

Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	1,80	1,00	1,245	1,70	1,00	1,101	1,75	1,00	1,166
Sólo entro en páginas web recomendadas para mi edad	2,82	3,00	1,600	3,37	3,00	1,358	3,11	3,00	1,494
Los chats públicos son páginas seguras donde nadie puede hacerme nada	2,44	2,00	1,387	2,26	2,00	1,188	2,35	2,00	1,282
No pasa nada por descargar música o aplicaciones "pirateadas"	3,06	3,00	1,346	3,02	3,00	1,232	3,04	3,00	1,281
Si conozco a alguien simpático/a jugando en red, le agregaría como 'amigo/a' en mi red social	2,32	2,00	1,269	2,39	2,00	1,373	2,36	2,00	1,319
Si una página web me pide el número de teléfono, se lo doy	1,72	1,00	1,179	1,72	1,00	1,114	1,72	1,00	1,139
Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	1,58	1,00	1,071	1,77	1,00	1,210	1,68	1,00	1,146
Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	2,12	2,00	1,272	1,77	1,00	1,239	1,93	1,00	1,261

Podemos apreciar que en el análisis descriptivo de las variables respecto al género existen diferencias, cuya significación se podrá apreciar, a continuación, en la prueba U de Mann-Whitney.

Tabla 77 Prueba U de Mann-Whitney escala de Likert

	U de Mann-Whitney	W de Wilcoxon	**Z**	**Sig. asintót. (bilateral)**
Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	**1361,500**	3014,500	**-,508**	**,612**
Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	**1392,000**	3045,000	**-,238**	**,812**
Sólo entro en páginas web recomendadas para mi edad	**1142,000**	2417,000	**-1,811**	**,070**
Los chats públicos son páginas seguras donde nadie puede hacerme nada	**1349,000**	3002,000	**-,493**	**,622**
No pasa nada por descargar música o aplicaciones "pirateadas"	**1421,500**	3074,500	**-,023**	**,982**
Si conozco a alguien simpático/a jugando en red, le agregaría como 'amigo/a' en mi red social	**1405,500**	2680,500	**-,126**	**,899**
Si una página web me pide el número de teléfono, se lo doy	**1387,500**	2662,500	**-,273**	**,785**
Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	**120**	2574,000	**-,946**	**,344**
Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	**1154,000**	2807,000	**-1,874**	**,061**

a. Variable de agrupación: Género

No se aprecian diferencias significativas respecto al género de las variables que utilizan escala Likert. No obstante, podemos observar que los resultados obtenidos de aquellas personas que afirman 'Solo entrar en páginas web adaptadas a su edad' y las

que consideran que ‘Insultar, o vacilar, a un/a compañero/a en una red social es menos humillante que decírselo en persona’ tienen tendencia a mostrar resultados significativos entre hombres y mujeres. Ésta hipótesis podría darse en caso que la muestra fuese de mayor tamaño. No obstante, en nuestra muestra se concluye que no son significativas.

2.1.2. Análisis de la influencia de la variable Información previa hábitos seguros y responsables

Se evalúa si hay diferencias significativas en los hábitos seguros y responsables en el uso de las TIC entre los adolescentes que han recibido información sobre hábitos seguros y responsables en el uso de las TIC y los que no la han recibido.

Contactos en RRSS

Tabla 78 Contingencia contactos en RRSS

			Información previa hábitos seguros y responsables		Total
			No	Si	
¿A quién aceptarías como ‘amigo’ en tus redes sociales?	A mis amigos	Recuento	31	24	55
		% Información previa hábitos seguros y responsables	68,9%	38,7%	51,4%
	A mis amigos y a amigos de mis amigos	Recuento	5	22	27
		% Información previa hábitos seguros y responsables	11,1%	35,5%	25,2%
	A mis amigos, a amigos de mis amigos y a personas que conozco en internet	Recuento	6	11	17
		% Información previa hábitos seguros y responsables	13,3%	17,7%	15,9%

	A todo el mundo que me lo proponga	Recuento	3	5	8
		% Información previa hábitos seguros y responsables	6,7%	8,1%	7,5%
Total		Recuento	45	62	107
		% Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 79 Prueba Chi-cuadrado contactos en RRSS

				Sig. de Monte Carlo (bilateral)		
	Valor	Gl	Sig. asintótica (bilateral)	Sig.	Intervalo de confianza al 99%	
					Límite inferior	Límite superior
Chi-cuadrado de Pearson	11,146[a]	3	,011	,010	,008	,013
Razón de verosimilitudes	11,734	3	,008	,013	,010	,016
Estadístico exacto de Fisher	11,300			,010	,007	,013
Asociación lineal por lineal	3,883[c]	1	,049	,057	,051	,063
N de casos válidos	107					

El haber recibido o no información previa sobre los hábitos seguros y responsables en el uso de las TIC está asociado con las personas que agregan los jóvenes a sus redes sociales (Chi-cuadrado: 11,146; gl = 3; p= 0,011), donde la prueba de Monte Carlo obtiene p=0,010.

Fotos personales compartidas en RRSS

Tabla 80 Informe fotos personales compartidas en RRSS

Información previa hábitos seguros y responsables

	No			Sí			Total		
	Media	Mediana	Desv. típ.	Media	Mediana	Desv. típ.	Media	Mediana	Desv. típ.
¿Cuántas fotos, en las que apareces, tienes subidas a tus redes sociales?	2,04	2,00	1,313	2,31	2,00	1,288	2,20	2,00	1,299

Tabla 81 Prueba U de Mann-Whitney fotos compartidas en RRSS

	U de Mann-Whitney	W de Wilcoxon	**Z**	**Sig. asintót. (bilateral)**
¿Cuántas fotos, en las que apareces, tienes subidas a tus redes sociales?	**1218,000**	2253,000	**-1,157**	**,247**

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable fotos compartidas en RRSS (U-MW: 1218; z = -1,157; p= 0,247).

Percepción fotos inadecuadas en RRSS

Tabla 82 Contingencia percepción fotos inadecuadas en RRSS

			Información previa hábitos seguros y responsables		Total
			No	Sí	
Alguna de las fotos, en las que apareces, que tienes compartidas en tus redes sociales, ¿podría parecerles inadecuada a tus padres si la vieran?	No	Recuento	38	55	93
		% dentro de Información previa hábitos seguros y responsables	90,5%	91,7%	91,2%
	Sí	Recuento	4	5	9
		% dentro de Información previa hábitos seguros y responsables	9,5%	8,3%	8,8%

Total	Recuento	42	60	102
	% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 83 Pruebas de chi-cuadrado percepción fotos inadecuadas en RRSS

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,044[a]**	**1**	,835		
Corrección por continuidad[b]	,000	1	1,000		
Razón de verosimilitudes	,043	1	,835		
Estadístico exacto de Fisher				**1,000**	,551
Asociación lineal por lineal	,043	1	,836		
N de casos válidos	102				

a. **1 casillas (25,0%)** tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 3,71.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable fotos inadecuadas (Chi-cuadrado: 0,044; gl = 1; p= 0,835). El 25% de los casos tienen una frecuencia esperada inferior a 5 por lo que observamos el estadístico exacto de Fischer que corrobora la no significación al obtener 1,000.

Percepción comentario inadecuado en RRSS

Tabla 84 Contingencia percepción comentario inadecuado en RRSS

		Información previa hábitos seguros y responsables		Total
		No	Sí	
¿Alguno de los comentarios, que No	Recuento	30	48	78

tienes en tus redes sociales, podría parecerles inadecuado a tus padres si lo vieran?	Sí	% dentro de Información previa hábitos seguros y responsables	71,4%	80,0%	76,5%
		Recuento	12	12	24
		% dentro de Información previa hábitos seguros y responsables	28,6%	20,0%	23,5%
Total		Recuento	42	60	102
		% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 85 Pruebas de chi-cuadrado percepción comentario inadecuado en RRSS

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**1,009[a]**	**1**	**,315**		
Corrección por continuidad[b]	,589	1	,443		
Razón de verosimilitudes	,998	1	,318		
Estadístico exacto de Fisher				,349	,221
Asociación lineal por lineal	,999	1	,318		
N de casos válidos	102				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 9,88.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable comentarios inadecuados (Chi-cuadrado: 1,009; gl = 1; p= 0,315).

Configuración seguridad y privacidad en RRSS

Tabla 86 Contingencia configuración seguridad y privacidad en RRSS

		Información previa hábitos seguros y responsables	Total

			No	Sí	
¿Consideras necesario configurar tú mismo/a la seguridad y privacidad de tus redes sociales?	No	Recuento	25	31	56
		% dentro de Información previa hábitos seguros y responsables	58,1%	50,8%	53,8%
	Sí	Recuento	18	30	48
		% dentro de Información previa hábitos seguros y responsables	41,9%	49,2%	46,2%
Total		Recuento	43	61	104
		% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 87 Pruebas de chi-cuadrado configuración seguridad y privacidad en RRSS

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,544[a]**	**1**	**,461**		
Corrección por continuidad [b]	,289	1	,591		
Razón de verosimilitudes	,545	1	,460		
Estadístico exacto de Fisher				,550	,296
Asociación lineal por lineal	,539	1	,463		
N de casos válidos	104				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 19,85.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable configurar privacidad (Chi-cuadrado: 0,554; gl = 1; p= 0,461).

Predisposición a compartir fotos o vídeos personales con amigos

Tabla 88 Contingencia predisposición a compartir fotos o vídeos personales con amigos

			Información previa hábitos seguros y responsables		Total
			No	Sí	
PRETEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con mis amigos]	No	Recuento	2	6	8
		% dentro de Información previa hábitos seguros y responsables	4,4%	9,7%	7,5%
	Sí	Recuento	43	56	99
		% dentro de Información previa hábitos seguros y responsables	95,6%	90,3%	92,5%
Total		Recuento	45	62	107
		% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 89 Pruebas de chi-cuadrado predisposición a compartir fotos o vídeos personales con amigos

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**1,032**[a]	**1**	,310		
Corrección por continuidad[b]	,414	1	,520		
Razón de verosimilitudes	1,093	1	,296		
Estadístico exacto de Fisher				**,463**	,265
Asociación lineal por lineal	1,023	1	,312		
N de casos válidos	107				

a**. 2 casillas (50,0%)** tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 3,36.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable fotos con mis amigos (Chi-cuadrado: 1,032; gl = 1; p= 0,310). El 50% de los casos tienen una frecuencia esperada inferior a 5 por lo que

observamos el estadístico exacto de Fischer que corrobora que no hay diferencias significativas entre las variables analizadas, al obtener 1,000.

Predisposición a compartir fotos o vídeos personales con amigos de mis amigos

Tabla 90 Contingencia predisposición a compartir fotos o vídeos personales con amigos de mis amigos

			Información previa hábitos seguros y responsables		Total
			No	Sí	
PRETEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con amigos de mis amigos]	No	Recuento	18	28	46
		% dentro de Información previa hábitos seguros y responsables	40,0%	45,2%	43,0%
	Sí	Recuento	27	34	61
		% dentro de Información previa hábitos seguros y responsables	60,0%	54,8%	57,0%
Total		Recuento	45	62	107
		% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 91 Pruebas de chi-cuadrado predisposición a compartir fotos o vídeos personales con amigos de mis amigos

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,283[a]**	**1**	**,594**		
Corrección por continuidad [b]	,112	1	,738		
Razón de verosimilitudes	,284	1	,594		
Estadístico exacto de Fisher				,693	,370
Asociación lineal por lineal	,281	1	,596		
N de casos válidos	107				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 19,35.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable fotos con amigos de mis amigos (Chi-cuadrado: 0,283; gl = 1; p= 0,594).

Predisposición a compartir fotos o vídeos personales con personas conocidas en internet

Tabla 92 Contingencia predisposición a compartir fotos o vídeos personales con personas conocidas en internet

			Información previa hábitos seguros y responsables		Total
			No	Sí	
PRETEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con personas que he conocido en internet]	No	Recuento	30	46	76
		% dentro de Información previa hábitos seguros y responsables	66,7%	74,2%	71,0%
	Sí	Recuento	15	16	31
		% dentro de Información previa hábitos seguros y responsables	33,3%	25,8%	29,0%
Total		Recuento	45	62	107
		% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 93 Pruebas de chi-cuadrado predisposición a compartir fotos o vídeos personales con personas conocidas en internet

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,718[a]**	**1**	**,397**		
Corrección por continuidad[b]	,399	1	,528		
Razón de verosimilitudes	,714	1	,398		
Estadístico exacto de Fisher				,518	,263
Asociación lineal por lineal	,711	1	,399		

N de casos válidos	107

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 13,04.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable fotos con personas conocidas en internet (Chi-cuadrado: 0,718; gl = 1; p= 0,397).

Predisposición a compartir el e-mail con desconocidos

Tabla 94 Contingencia predisposición a compartir el e-mail con desconocidos

			Información previa hábitos seguros y responsables		Total
			No	Sí	
PRETEST ¿Qué tipo de información compartirías con personas conocidas en internet? [e-mail]	No	Recuento	38	57	95
		% dentro de Información previa hábitos seguros y responsables	84,4%	91,9%	88,8%
	Sí	Recuento	7	5	12
		% dentro de Información previa hábitos seguros y responsables	15,6%	8,1%	11,2%
Total		Recuento	45	45	62
		% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 95 Prueba chi-cuadrado predisposición a compartir el e-mail con desconocidos

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	1,469a	1	,225		
Corrección por continuidad[b]	,813	1	,367		
Razón de verosimilitudes	1,448	1	,229		
Estadístico exacto de Fisher				,352	,183
Asociación lineal por lineal	1,456	1	,228		
N de casos válidos	107				

a. 2 casillas (50,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 1,10.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable webcam con amigos (Chi-cuadrado: 1,469; gl = 1; p= 0,225), donde el estadístico exacto de Fisher es 0,352.

Predisposición a compartir el teléfono con desconocidos

Tabla 96 Contingencia predisposición a compartir el teléfono con desconocidos

			Información previa hábitos seguros y responsables		Total
			No	Sí	
¿Qué tipo de información compartirías con personas conocidas en internet? [teléfono]	No	Recuento	41	53	94
		% dentro de Información previa hábitos seguros y responsables	91,1%	85,5%	87,9%
	Sí	Recuento	4	9	13
		% dentro de Información previa hábitos seguros y responsables	8,9%	14,5%	12,1%
Total		Recuento	45	45	62
		% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 97 Prueba chi-cuadrado predisposición a compartir el teléfono con desconocidos

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	,774a	1	,379	,551	,285
Corrección por continuidad[b]	,336	1	,562		
Razón de verosimilitudes	,797	1	,372	,551	,285
Estadístico exacto de Fisher				,551	,285
Asociación lineal por lineal	,766d	1	,381	,551	,285
N de casos válidos	107				

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable compartir teléfono con desconocidos (Chi-cuadrado: 0,774; gl = 1; p= 0,379), donde el estadístico exacto de Fisher es 0,551.

Predisposición uso de la webcam con mis amigos

Tabla 98 Contingencia predisposición uso de la webcam con mis amigos

			Información previa hábitos seguros y responsables		Total
			No	Sí	
De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con mis amigos]	No	Recuento	24	28	52
		% dentro de Información previa hábitos seguros y responsables	53,3%	45,2%	48,6%
	Sí	Recuento	21	34	55
		% dentro de Información previa hábitos seguros y responsables	46,7%	54,8%	51,4%
Total		Recuento	45	62	107
		% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 99 Pruebas de chi-cuadrado predisposición uso de la webcam con mis amigos

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,697[a]**	**1**	**,404**		
Corrección por continuidad[b]	,408	1	,523		
Razón de verosimilitudes	,698	1	,404		
Estadístico exacto de Fisher				,438	,261
Asociación lineal por lineal	,691	1	,406		
N de casos válidos	107				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 21,87.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable webcam con amigos (Chi-cuadrado: 0,697; gl = 1; p= 0,404).

Predisposición uso de la webcam con amigos de mis amigos

Tabla 100 Contingencia predisposición uso de la webcam con amigos de mis amigos

			Información previa hábitos seguros y responsables		Total
			No	Sí	
De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con amigos de mis amigos]	No	Recuento	41	54	95
		% dentro de Información previa hábitos seguros y responsables	91,1%	87,1%	88,8%
	Sí	Recuento	4	8	12
		% dentro de Información previa hábitos seguros y responsables	8,9%	12,9%	11,2%
Total		Recuento	45	62	107

	% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 101 Pruebas de chi-cuadrado predisposición uso de la webcam con amigos de mis amigos

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,422[a]**	**1**	**,516**		
Corrección por continuidad[b]	,115	1	,734		
Razón de verosimilitudes	,431	1	,511		
Estadístico exacto de Fisher				,758	,372
Asociación lineal por lineal	,418	1	,518		
N de casos válidos	107				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 5,05.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable webcam con amigos de mis amigos (Chi-cuadrado: 0,422; gl = 1; p= 0,516).

Predisposición uso de la webcam con conocidos en internet

Tabla 102 Contingencia predisposición uso de la webcam con conocidos en internet

			Información previa hábitos seguros y responsables		Total
			No	Sí	
PRETEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Conocidos en internet]	No	Recuento	44	59	103
		% dentro de Información previa hábitos seguros y responsables	97,8%	95,2%	96,3%
	Sí	Recuento	1	3	4
		% dentro de Información previa hábitos seguros y responsables	2,2%	4,8%	3,7%

Total	Recuento	45	62	107
	% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 103 Pruebas de chi-cuadrado predisposición uso de la webcam con conocidos en internet

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,496**[a]	**1**	,481		
Corrección por continuidad[b]	,035	1	,851		
Razón de verosimilitudes	,526	1	,468		
Estadístico exacto de Fisher				**,637**	,438
Asociación lineal por lineal	,491	1	,483		
N de casos válidos	107				

a. **2 casillas (50,0%)** tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 1,68.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable webcam con conocidos en internet (Chi-cuadrado: 4,96; gl = 1; p= 0,481). El 50% de los casos tienen una frecuencia esperada inferior a 5 por lo que observamos el estadístico exacto de Fischer que corrobora que no hay diferencias significativas entre las variables analizadas, al obtener p=1,000.

Humillación a terceros en RRSS

Tabla 104 Contingencia humillación a terceros en RRSS

		Información previa hábitos seguros y responsables		Total
		No	Sí	

¿Alguna vez te has burlado de un comentario o foto en una red social?	No	Recuento	16	39	55
		% dentro de Información previa hábitos seguros y responsables	38,1%	62,9%	52,9%
	Sí	Recuento	26	23	49
		% dentro de Información previa hábitos seguros y responsables	61,9%	37,1%	47,1%
Total		Recuento	42	62	104
		% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 105 Pruebas de chi-cuadrado humillación a terceros en RRSS

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**6,184[a]**	**1**	**,013**		
Corrección por continuidad[b]	5,229	1	,022		
Razón de verosimilitudes	6,234	1	,013		
Estadístico exacto de Fisher				,017	,011
Asociación lineal por lineal	6,125	1	,013		
N de casos válidos	104				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 19,79.

b. Calculado sólo para una tabla de 2x2.

Se hallan diferencias significativas entre los adolescentes que recibieron una información previa sobre hábitos seguros y responsables y quienes no han recibido dicha información, respecto a la variable burlarse de una foto o comentario en la red (Chi-cuadrado: 6,184; gl: 1; p=0,013). Los adolescentes que recibieron información sobre hábitos seguros y responsables dicen mayoritariamente que NO, 62.9%, se han burlado nunca de una foto o comentario, mientras que los que no recibieron la información contestan mayoritariamente que SÍ lo han hecho, 61,9%.

Uso de software de protección en el ordenador

Tabla 106 Contingencia uso de software de protección en el ordenador

			Información previa hábitos seguros y responsables		Total
			No	Sí	
Tienes instalado software de protección, como por ejemplo un antivirus, en tu ordenador de casa?	No	Recuento	7	7	14
		% dentro de Información previa hábitos seguros y responsables	16,7%	11,9%	13,9%
	Sí	Recuento	35	52	87
		% dentro de Información previa hábitos seguros y responsables	83,3%	88,1%	86,1%
Total		Recuento	42	59	101
		% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 107 Pruebas de chi-cuadrado uso de software de protección en el ordenador

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**,474[a]**	**1**	**,491**		
Corrección por continuidad[b]	,157	1	,692		
Razón de verosimilitudes	,468	1	,494		
Estadístico exacto de Fisher				,565	,343
Asociación lineal por lineal	,469	1	,493		
N de casos válidos	101				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 5,82.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable antivirus ordenador (Chi-cuadrado: 0,474; gl = 1; p= 0,491).

Uso de software de protección en el Smartphone

Tabla 108 Contingencia uso de software de protección en el Smartphone

			Información previa hábitos seguros y responsables		Total
			No	Sí	
¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu Smartphone?	No	Recuento	20	17	37
		% dentro de Información previa hábitos seguros y responsables	51,3%	32,1%	40,2%
	Sí	Recuento	19	36	55
		% dentro de Información previa hábitos seguros y responsables	48,7%	67,9%	59,8%
Total		Recuento	39	53	92
		% dentro de Información previa hábitos seguros y responsables	100,0%	100,0%	100,0%

Tabla 109 Pruebas de chi-cuadrado uso de software de protección en el Smartphone

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	**3,447[a]**	**1**	**,063**		
Corrección por continuidad[b]	2,695	1	,101		
Razón de verosimilitudes	3,446	1	,063		
Estadístico exacto de Fisher				,086	,050
Asociación lineal por lineal	3,410	1	,065		
N de casos válidos	92				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 15,68.

b. Calculado sólo para una tabla de 2x2.

No se hallan diferencias significativas, entre los jóvenes que han recibido información previa sobre hábitos seguros y responsables y aquellos que no la han recibido, respecto a la variable antivirus Smartphone (Chi-cuadrado: 3,447; gl = 1; p= 0,063).

No obstante, los resultados obtenidos muestran que el cruce de las variables están bastante cerca de ser significativas, por lo que de tratarse de una muestra mayor podría concluir que existe significación. Podemos observar que el 67,9% de los adolescentes que recibieron información sobre hábitos seguros y responsables tienen instalado software de protección en su ordenador de casa, mientras, que los que no han recibido información lo utilizan el 48,7%.

Variables que utilizan la escala Likert

A continuación, como hemos podido comprobar para analizar las variables que utilizan una escala Likert, debido a que no siguen una distribución normal, es necesario aplicar la prueba U de Mann-Whitney para analizar las diferencias entre quienes recibieron o no información sobre hábitos seguros y responsables en el uso de las TIC.

Tabla 110 Estadísticos descriptivos variables escala Likert

	Información previa hábitos seguros y responsables								
	No			Sí			Total		
	Media	Mediana	Desv. típ.	Media	Mediana	Desv. típ.	Media	Mediana	Desv. típ.
Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	4,36	5,00	1,131	4,63	5,00	,773	4,51	5,00	,945
Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	1,98	1,00	1,438	1,58	1,00	,897	1,75	1,00	1,166

Sólo entro en páginas web recomendadas para mi edad	3,00	3,00	1,508	3,19	3,00	1,491	3,11	3,00	1,494
Los chats públicos son páginas seguras donde nadie puede hacerme nada	2,33	2,00	1,279	2,35	2,00	1,294	2,35	2,00	1,282
No pasa nada por descargar música o aplicaciones "pirateadas"	3,18	3,00	1,267	2,94	3,00	1,291	3,04	3,00	1,281
Si conozco a alguien simpático/a jugando en red, le agregaría como 'amigo/a' en mi red social	2,62	2,00	1,512	2,16	2,00	1,134	2,36	2,00	1,319
Si una página web me pide el número de teléfono, se lo doy	1,87	1,00	1,254	1,61	1,00	1,046	1,72	1,00	1,139
Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	1,93	1,00	1,355	1,50	1,00	,937	1,68	1,00	1,146
Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	2,18	2,00	1,336	1,76	1,00	1,183	1,93	1,00	1,261

Tabla 111 Prueba U de Mann-Whitney variables escala Likert

	U de Mann-Whitney	W de Wilcoxon	**Z**	**Sig. asintót. (bilateral)**
Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	**1236,000**	2271,000	**-1,285**	**,199**

Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	**1260,000**	3213,000	**-,984**	**,325**
Sólo entro en páginas web recomendadas para mi edad	**1293,000**	2328,000	**-,660**	**,510**
Los chats públicos son páginas seguras donde nadie puede hacerme nada	**1383,000**	2418,000	**-,079**	**,937**
No pasa nada por descargar música o aplicaciones "pirateadas"	**1250,000**	3203,000	**-,945**	**,345**
Si conozco a alguien simpático/a jugando en red, le agregaría como 'amigo/a' en mi red social	**1180,000**	3133,000	**-1,408**	**,159**
Si una página web me pide el número de teléfono, se lo doy	**1269,500**	3222,500	**-,922**	**,357**
Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	**1211,000**	3164,000	**-1,396**	**,163**
Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	**1140,000**	3093,000	**-1,782**	**,075**

a. Variable de agrupación: Información previa hábitos seguros y responsables

No hay diferencias significativas en los hábitos de uso seguro de internet entre quienes recibieron información sobre hábitos seguros y responsables y quienes no la recibieron. La única variable que podría ser significativa en muestras mayores es 'Insultar, o vacilar, a un compañero/a o amigo/a en una red social es menos humillante que decírselo en persona' dado que el estadístico Z ha salido bastante bajo por lo que podría ser significativa de tratarse de una muestra mayor.

2.2. Síntesis del análisis de los resultados del pretest

El pretest, que fue contestado por el grupo de control y el grupo experimental, nos permite conocer la exposición de los participantes a los riesgos incluidos en el estudio.

Los resultados que expondremos a continuación, nos permiten conocer los riesgos a los que se exponen los jóvenes al utilizan las TIC, previamente a la implementación de la intervención con el grupo experimental. Esto nos permite dar respuesta a la hipótesis 1 e hipótesis 2 dado que aún no hemos influido en los grupos que forman parte del estudio.

Resultados significativos del pretest: total de la muestra

- El 42,1% no han recibido información sobre hábitos seguros y responsables en el uso de las TIC. Ver **Tabla 6.** La falta de información y formación en hábitos seguros y responsables en el uso de las TIC, expone a los jóvenes a todos los riesgos que hemos examinado.

- El 53,8% no consideran necesario ser ellos mismos quienes configuren la seguridad y privacidad de sus redes sociales. Ver **Tabla 16**. Esta situación deja la seguridad y privacidad de la información personal de los jóvenes en manos de las empresas desarrolladoras de la aplicación, quienes permitirán acceder a la información de sus usuarios a quienes consideren oportuno, siguiendo sus criterios de beneficio empresarial.

- El 29% compartirían fotos personales con personas conocidas en internet. Ver **Tabla 22.** Además, el 11,2% afirman que compartirían su número

de teléfono con personas conocidas en internet (véase **Tabla 26**). Hemos podido apreciar los riesgos de la exposición de información personal a través de la red, como por puede ser el ciberbulling. Dependiendo del contenido de las imágenes personales también podría exponerse a sextorsión, cibergrooming, etc.

- El 8,8% afirman tener fotos compartidas que podrían parecerles inadecuadas a sus padres. Ver **Tabla 12**. Esta variable, como hemos comentado, nos aporta información sobre la calidad de las fotos que tienen los jóvenes compartidas en sus redes sociales.

- El 23,5% afirman que han hecho comentarios a través de redes sociales que podrían parecerles inadecuados a sus padres. Ver **Tabla 14**. De igual forma que en la pregunta anterior, la variables nos permite obtener información sobre la calidad de los contenidos compartidos, en éste caso, sobre los comentarios realizados en las redes sociales.

- El 51,4% utilizarían la webcam con amigos (véase

-

-

- ***Tabla 29***), el 11,2% con amigos de amigos (véase **Tabla 31**) y el 3,7% con conocidos en internet (véase **Tabla 33**). Los riesgos derivados del uso de la webcam pueden ser diversos dependiendo del objetivo de uso y de la persona con la que se utiliza.

- El 13,9% no disponen de software de protección en el ordenador (véase **Tabla 37**) y el 40,2% no lo tienen instalado en el smartphone (véase **Tabla 39**). El software de protección se ha convertido en una herramienta imprescindible en los dispositivos de conexión a internet. La existencia de

software dirigido al robo o copia de información personal representa un grave peligro por las consecuencias que pueden desencadenar, por lo que es necesario la protección de los dispositivos.

- Es significativo la proporción de jóvenes que afirman haberse burlado de un comentario o foto a través de las redes sociales, que asciende al 47,1% de la muestra. Ver **Tabla 35**

- La **Tabla 41** nos muestra las variables medidas con una escala Likert del 1 al 5 que nos permiten conocer el nivel de acuerdo con las afirmaciones planteadas y el número de fotos personales que tienen compartidas los jóvenes a través de sus redes sociales cuyas opciones de respuesta están divididas en 5 rangos.

En cada afirmación, se puede observar la información descriptiva de las respuestas obtenidas. Compartir información personal con personas conocidas a través de la red, el acceso a páginas no adaptadas a la edad de los jóvenes, la percepción de seguridad en páginas que facilitan el contacto con personas desconocidas, la percepción sobre las descargas ilegales, etc., muestran unos hábitos aún lejos de los hábitos seguros y responsables deseables que eviten a los jóvenes exponerse a los riesgos derivados de las TIC.

Por tanto, se concluye que los jóvenes se exponen a los riesgos analizados de manera desigual según los riesgos a los que nos referimos. Las acciones encaminadas en el desarrollo de los hábitos seguros y responsables en el uso de las TIC no han conseguido evitar que los jóvenes se expongan a los riesgos derivados de su uso por lo que se valora necesario la implementación de nuevos planes de intervención y protección de los menores al utilizar las TIC.

Análisis de la variable género como variable independiente en el pretest

En éste apartado, explicaremos las conclusiones halladas de la asociación del género con las variables estudiadas, anteriormente a la implementación de la intervención. De este modo, daremos respuesta a la hipótesis 5.

El análisis de las variables que forman parte de la escala Likert, resultan no significativas en función del género, sin embargo, como podemos apreciar en la **Tabla 76** que muestra el informe obtenido con los estadísticos descriptivos, tenemos variables que ofrecen resultados diversos en función del riesgo que se evalúa.

La prueba U de Mann-Whitney nos confirma la asociación entre el género y las variables analizadas, en el siguiente caso:

- Fotos compartidas en redes sociales: los resultados obtenidos en la **Tabla 47** muestran la existencia de diferencias significativas entre hombres y mujeres respecto al número de fotos que los jóvenes tienen subidas a sus redes sociales (U de M-W: 922: Z= -3,252; p=0,001), siendo las mujeres quienes disponen de más información de este tipo en sus redes sociales. La mediana que se obtiene en el caso de los hombres es de 1,5 y de 2 en el caso de mujeres (véase **Tabla 46**).

Además, podemos observar en la **Tabla 77** que existen resultados que se aproximan a la significación. Las opciones de respuesta ofrecen una escala Likert de 1 a 5, que fluctúa entre totalmente en desacuerdo con la afirmación planteada a totalmente de acuerdo. Nos referimos a los siguientes casos:

- Las personas que afirman 'Solo entrar en páginas web adaptadas a su edad' difiere en función del género, obteniendo una media 2,82 y 3,37, con la misma mediana, correspondiendo a hombres y mujeres respectivamente. La U de Mann-Whitney obtiene (U de M-W: 1142: Z= -1,811; p=0,070).

- La percepción de la humillación valorada a través del ítem: 'Insultar, o vacilar, a un/a compañero/a en una red social es menos humillante que decírselo en persona', obtiene una media de 2,12 y una mediana de 2, en el caso de los hombres y una media de 1,77 y mediana 1, si nos referimos a las mujeres. La U de Mann-Whitney obtiene (U de M-W: 1154: Z= -1,874; p=0,061).

La p de Mann-Whitney nos confirma que no existe significación aunque podría ser significativa en muestras de mayor tamaño.

Análisis de la variable 'Información previa sobre hábitos seguros y responsables en el uso de las TIC' como variable independiente

Los jóvenes que han recibido información sobre hábitos seguros y responsables en el uso de las TIC podrían exponerse en menor medida a los riesgos derivados de las TIC que los jóvenes que no la han recibido. Sin embargo, los resultados hallados ponen en duda su eficacia en la reducción de la exposición a riesgos.

No obstante, se obtienen algunos resultados que se ve conveniente comentar:

- Los jóvenes que han recibido información sobre hábitos seguros y responsables en el uso de internet, permiten el acceso a sus redes sociales a personas

más cercanas y conocidas que los que nunca han recibido información de este tipo. En la **Tabla 78** se observa que las diferencias entre aquellos que la han recibido y los que no lo han hecho, es significativa respecto a la variable contactos en RRSS.

- Respecto a la pregunta: ¿Alguna vez te has burlado de un comentario o foto en una red social?, el 62,9% de las personas que han recibido información respondieron 'No', mientras que de las personas que no han recibido información tan sólo el 38,1% respondieron 'No', concluyéndose la significación de la asociación entre ambas variables (Chi-cuadrado: 6,184; gl: 1; p=0,013). Ver **Tabla 105**

- De las personas que tienen instalado software de protección en sus Smartphones, el 67,9% forman parte del grupo de personas que han recibido información. Sin embargo, la p de chi-cuadrado concluye que no existe significación aunque se aproxima con un p=0,063. Por tanto, en muestras de mayor tamaño podría ser significativa. Ver **Tabla 108**

- En el informe estadístico descriptivo de las variables que utilizan la escala Likert se puede apreciar que existen diferencias en la percepción de insultar, o vacilar a otras personas en una red social es menos humillante respecto al mismo hecho realizado en persona (véase **Tabla 110**). No obstante, de igual manera que en el punto anterior no se demuestra la asociación entre ambas variables aunque se aproxima a la significación, por lo que en muestras mayores podría ser significativa (U de M-W:1140; Z=-1,782; p=0,075). Ver **Tabla 111.**

Por tanto, hemos podido apreciar que los resultados obtenidos del cruce de la variable 'información previa hábitos seguros y responsables', con el resto de variables del estudio, es en la mayor parte de los casos como no significativa.

3. Fase Postest: Impacto del plan de intervención

En esta fase conoceremos el impacto que ha tenido el plan de intervención implementado sobre los hábitos seguros y responsables de los jóvenes que forman parte del estudio.

3.1. Análisis de las diferencias entre el pretest y el postest

El objetivo de este análisis es evaluar los resultados obtenidos en la intervención. El grupo experimental fue expuesto a un tratamiento con el objetivo de favorecer el desarrollo de los hábitos seguros y responsables en uso de las TIC. El grupo de control por su parte no ha recibido dicho tratamiento, por lo que cualquier cambio en sus hábitos se debe a causas ajenas a la intervención. Por lo tanto, se espera que la intervención contribuya a disminuir la exposición a los riesgos derivados del uso de las TIC, contribuyendo al desarrollo de sus hábitos seguros y responsables. Si esto se cumple, se deberían hallar diferencias significativas entre el pretest y el postest del grupo experimental y diferencias en el postest entre el grupo experimental y el de control. Se supone que los otros factores no han cambiado, y si lo han hecho al ser los mismos sujetos medidos antes y después de la intervención el cambio de dichas variables no influiría en los hábitos en uso seguro y responsable de las TIC. Por tanto, los cambios pueden ser atribuidos a la intervención.

A continuación se muestran los resultados de la comparación de la medición antes y después de la intervención de los grupos experimental y de control. Para ello, se ha empleado la prueba Wilcoxon en las variables ordinales no dicotómicas y el estadístico de McNemar que nos permite analizar los cambios experimentados en las

variables dicotómicas, obteniendo los sujetos que han cambiado su respuesta respecto al cuestionario pretest. Es decir, contabiliza los sujetos que respondieron en el pretest 'sí', a la pregunta en análisis, y en postest han seleccionado la opción de respuesta 'no', y viceversa. La prueba de McNemar se utiliza para decidir si puede o no aceptarse que determinado "tratamiento" induce un cambio en la respuesta dicotómica o dicotomizada de los elementos sometidos al mismo, y es aplicable a los diseños del tipo "antes-después" en los que cada elemento actúa como su propio control.

Contactos en RRSS

Tabla 112 Informe descriptivo impacto contactos en RRSS

Grupo		¿A quién aceptarías como 'amigo' en tus redes sociales? Pretest	¿A quién aceptarías como 'amigo' en tus redes sociales? Postest
Colegio Control	Media	2,04	1,98
	Mediana	2,00	2,00
	Desv. típ.	,999	,965
	N	45	45
Colegio Experimental	Media	1,85	1,66
	Mediana	2,00	1,00
	Desv. típ.	,827	,957
	N	62	62

Tabla 113 Prueba Wilcoxon impacto contactos en RRSS

Grupo		A quién aceptarías como amigo en tus redes sociales
Colegio Control	Z	-,550[b]
	Sig. asintót. (bilateral)	,583

Colegio Experimental	Z	-1,220[b]
	Sig. asintót. (bilateral)	,223

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos positivos.

Podemos observar que las diferencias entre pretest y postest no son significativas, por lo que los cambios observados pueden deberse al azar.

A continuación, vamos a realizar tres análisis de McNemar; uno para el grupo experimental, otro para el grupo control y otro, por defecto, para el total, que muestra los resultados totales del grupo experimental y control en conjunto.

Fotos inadecuadas en RRSS

Tabla 114 Contingencia impacto percepción fotos inadecuadas en RRSS

	POSTEST			POSTEST Alguna de las fotos, en las que apareces, que tienes compartidas en tus redes sociales, ¿podría parecerles inadecuada a tus padres si la vieran?		Total
				No	Sí	
Colegio Control	PRETEST Alguna de las fotos, en las que apareces, que tienes compartidas en tus redes sociales, ¿podría parecerles inadecuada a tus padres si la vieran?	No	Recuento	29	3	32
			% del total	76,3%	7,9%	84,2%
		Sí	Recuento	3	3	6
			% del total	7,9%	7,9%	15,8%
	Total		Recuento	32	6	38
			% del total	84,2%	15,8%	100,0%
Colegio Experimental	PRETEST Alguna de las fotos, en las que apareces, que tienes compartidas en	No	Recuento	51	4	55
			% del total	89,5%	7,0%	96,5%
		Sí	Recuento	2	0	2

	tus redes sociales, ¿podría parecerles inadecuada a tus padres si la vieran?		% del total	3,5%	0,0%	3,5%
	Total		Recuento	53	4	57
			% del total	93,0%	7,0%	100,0%
	PRETEST Alguna de las fotos, en las que apareces, que tienes compartidas en tus redes sociales, ¿podría parecerles inadecuada a tus padres si la vieran?	No	Recuento	80	7	87
			% del total	84,2%	7,4%	91,6%
		Sí	Recuento	5	3	8
Total			% del total	5,3%	3,2%	8,4%
		Total	Recuento	85	10	95
			% del total	89,5%	10,5%	100,0%

Se puede observar, en el grupo de control, que las casillas b y c son iguales, es decir, es evidente que no existe un patrón en los cambios, por eso la p en la prueba de McNemar que vemos a continuación es 1. En el caso del grupo experimental se ven diferencias, pero no son estadísticamente significativas, por eso p de McNemar resulta no significativa.

Tabla 115 Chi-cuadrado fotos inadecuadas en RRSS

POSTEST		Valor	Sig. exacta (bilateral)
Colegio Control	Prueba de McNemar		1,000[a]
	N de casos válidos	38	
Colegio Experimental	Prueba de McNemar		,687[a]
	N de casos válidos	57	
Total	Prueba de McNemar		,774[a]
	N de casos válidos	95	

a. Utilizada la distribución binomial

Por tanto, según los resultados del test de McNemar no se aprecian diferencias significativas en los resultados del pretest y el postest, respecto a la pregunta ‘Alguna de

las fotos, en las que apareces, que tienes compartidas en tus redes sociales, ¿podría parecerles inadecuada a tus padres si la vieran?', en la muestra total (p=0,774), ni en el grupo de control (p=1,0) ni en el grupo experimental (p=0,687).

Percepción comentarios inadecuados

Tabla 116 Contingencia impacto en la percepción comentarios inadecuados en RRSS

	POSTEST			POSTEST ¿Alguno de los comentarios, que tienes en tus redes sociales, podría parecerles inadecuado a tus padres si lo vieran?		Total
				No	Sí	
Colegio Control	PRETEST ¿Alguno de los comentarios, que tienes en tus redes sociales, podría parecerles inadecuado a tus padres si lo vieran?	No	Recuento	17	7	24
			% del total	44,7%	18,4%	63,2%
		Sí	Recuento	10	4	14
			% del total	26,3%	10,5%	36,8%
	Total		Recuento	27	11	38
			% del total	71,1%	28,9%	100,0%
Colegio Experimental	PRETEST ¿Alguno de los comentarios, que tienes en tus redes sociales, podría parecerles inadecuado a tus padres si lo vieran?	No	Recuento	38	10	48
			% del total	66,7%	17,5%	84,2%
		Sí	Recuento	7	2	9
			% del total	12,3%	3,5%	15,8%
	Total		Recuento	45	12	57
			% del total	78,9%	21,1%	100,0%
Total	PRETEST ¿Alguno de los comentarios, que tienes en tus redes sociales, podría parecerles inadecuado a tus padres si lo vieran?	No	Recuento	55	17	72
			% del total	57,9%	17,9%	75,8%
		Sí	Recuento	17	6	23
			% del total	17,9%	6,3%	24,2%
	Total		Recuento	72	23	95
			% del total	75,8%	24,2%	100,0%

Tabla 117 Chi-cuadrado impacto percepción comentarios inadecuados en RRSS

POSTEST		Valor	Sig. exacta (bilateral)
Colegio Control	Prueba de McNemar		,629[a]
	N de casos válidos	38	
Colegio Experimental	Prueba de McNemar		,629[a]
	N de casos válidos	57	
Total	Prueba de McNemar		1,000[a]
	N de casos válidos	95	

a. Utilizada la distribución binomial

Según los resultados del test de McNemar no se aprecian diferencias significativas en los resultados del pretest y el postest respecto a tener la pregunta '¿Alguno de los comentarios, que tienes en tus redes sociales, podría parecerles inadecuado a tus padres si lo vieran?' en la muestra total (p=1,0), ni en el grupo de control (p=0,629) ni en el grupo experimental (p=0,629).

Configurar seguridad privada

Tabla 118 Contingencia impacto configuración seguridad y privacidad en RRSS

POSTEST				POSTEST ¿Consideras necesario configurar tú mismo/a la seguridad y privacidad de tus redes sociales?		Total
				No	Sí	
Colegio Control POST	PRETEST ¿Consideras necesario configurar tú mismo/a la seguridad y privacidad de tus redes sociales?	No	Recuento	8	11	19
			% del total	20,0%	27,5%	47,5%
		Sí	Recuento	12	9	21
			% del total	30,0%	22,5%	52,5%
	Total		Recuento	20	20	40
			% del total	50,0%	50,0%	100,0%
Colegio Experimental POST	PRETEST ¿Consideras necesario configurar tú	No	Recuento	5	29	34
			% del total	8,5%	49,2%	57,6%

	mismo/a la seguridad y privacidad de tus redes sociales?	Sí	Recuento	4	21	25
			% del total	6,8%	35,6%	42,4%
	Total		Recuento	9	50	59
			% del total	15,3%	84,7%	100,0%
	PRETEST ¿Consideras necesario configurar tú mismo/a la seguridad y privacidad de tus redes sociales?	No	Recuento	13	40	53
			% del total	13,1%	40,4%	53,5%
Total		Sí	Recuento	16	30	46
			% del total	16,2%	30,3%	46,5%
	Total		Recuento	29	70	99
			% del total	29,3%	70,7%	100,0%

Tabla 119 Chi-cuadrado impacto configuración seguridad y privacidad en RRSS

POSTEST		Valor	Sig. exacta (bilateral)
Colegio Control POST	Prueba de McNemar		1,000[a]
	N de casos válidos	40	
Colegio Experimental POST	Prueba de McNemar		,000[a]
	N de casos válidos	59	
Total	Prueba de McNemar		,002[a]
	N de casos válidos	99	

a. Utilizada la distribución binomial

Según los resultados del test de McNemar se aprecian diferencias significativas en los resultados del pretest y el postest respecto a tener la pregunta '¿Consideras necesario configurar tú mismo/a la seguridad y privacidad de tus redes sociales?' en la muestra total (p=0,002) y en el grupo experimental (p<0,001). Sin embargo, no se producen cambio en el grupo de control (p=1,0).

En la **Tabla 118** se puede apreciar que el 85,3% de los jóvenes que antes de la intervención no consideraban necesario configurar ellos mismos la seguridad y privacidad de sus redes sociales, tras la intervención si lo consideran necesario.

Predisposición a compartir fotos con amigos

Tabla 120 Contingencia predisposición a compartir fotos o vídeos personales con amigos

	POSTEST			POSTEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con mis amigos]		Total
				No	Sí	
Colegio Control	PRETEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con mis amigos]	No	Recuento	0	4	4
			% del total	0,0%	8,9%	8,9%
		Sí	Recuento	4	37	41
			% del total	8,9%	82,2%	91,1%
	Total		Recuento	4	41	45
			% del total	8,9%	91,1%	100,0%
Colegio Experimental	PRETEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con mis amigos]	No	Recuento	1	3	4
			% del total	1,6%	4,8%	6,5%
		Sí	Recuento	1	57	58
			% del total	1,6%	91,9%	93,5%
	Total		Recuento	2	60	62
			% del total	3,2%	96,8%	100,0%
Total	PRETEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con mis amigos]	No	Recuento	1	7	8
			% del total	0,9%	6,5%	7,5%
		Sí	Recuento	5	94	99
			% del total	4,7%	87,9%	92,5%
	Total		Recuento	6	101	107

			% del total	5,6%	94,4%	100,0%

Tabla 121 Chi-cuadrado impacto predisposición a compartir fotos o vídeos personales con amigos

POSTEST		Valor	Sig. exacta (bilateral)
Colegio Control	Prueba de McNemar		1,000[a]
	N de casos válidos	45	
Colegio Experimental	Prueba de McNemar		,625[a]
	N de casos válidos	62	
Total	Prueba de McNemar		,774[a]
	N de casos válidos	107	

a. Utilizada la distribución binomial

Según los resultados del test de McNemar no se aprecian diferencias significativas en los resultados del pretest y el postest respecto a tener la pregunta 'De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con mis amigos]' en la muestra total (p=0,774), ni en el grupo de control (p=1,0) ni en el grupo experimental (p=0,625).

Predisposición a compartir foto o vídeos con amigos de mis amigos

Tabla 122 Contingencia predisposición a compartir fotos o vídeos personales con amigos de amigos

POSTEST				POSTEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con amigos de mis amigos]		Total
				No	Sí	
Colegio Control	PRETEST De las siguientes 'personas', ¿con quienes compartirías una	No	Recuento	10	9	19
			% del total	22,2%	20,0%	42,2%
		Sí	Recuento	9	17	26

	foto o vídeo en el que aparezcas? [Con amigos de mis amigos]		% del total	20,0%	37,8%	57,8%
	Total		Recuento	19	26	45
			% del total	42,2%	57,8%	100,0%
	PRETEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con amigos de mis amigos]	No	Recuento	13	14	27
			% del total	21,0%	22,6%	43,5%
		Sí	Recuento	18	17	35
Colegio Experimental			% del total	29,0%	27,4%	56,5%
	Total		Recuento	31	31	62
			% del total	50,0%	50,0%	100,0%
	PRETEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con amigos de mis amigos]	No	Recuento	23	23	46
			% del total	21,5%	21,5%	43,0%
		Sí	Recuento	27	34	61
Total			% del total	25,2%	31,8%	57,0%
	Total		Recuento	50	57	107
			% del total	46,7%	53,3%	100,0%

Tabla 123 Pruebas de chi-cuadrado predisposición a compartir fotos o vídeos personales con amigos de amigos

POSTEST		Valor	Sig. exacta (bilateral)
Colegio Control	Prueba de McNemar		1,000[a]
	N de casos válidos	45	
Colegio Experimental	Prueba de McNemar		,597[a]
	N de casos válidos	62	
Total	Prueba de McNemar		,672[a]
	N de casos válidos	107	

a. Utilizada la distribución binomial

Según los resultados del test de McNemar no se aprecian diferencias significativas en los resultados del pretest y el postest respecto a tener la pregunta ‘De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que

aparezcas? [Con amigos mis amigos]' en la muestra total (p=0,672), ni en el grupo de control (p=1,0) ni en el grupo experimental (p=0,597).

Predisposición a compartir fotos o vídeos con conocidos por internet

Tabla 124 Contingencia predisposición a compartir fotos o vídeos personales con conocidos en internet

	POSTEST			POSTEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con personas que he conocido en internet]		Total
				No	Sí	
Colegio Control	PRETEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con personas que he conocido en internet]	No	Recuento	27	3	30
			% del total	60,0%	6,7%	66,7%
		Sí	Recuento	5	10	15
			% del total	11,1%	22,2%	33,3%
	Total		Recuento	32	13	45
			% del total	71,1%	28,9%	100,0%
Colegio Experimental	PRETEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con personas que he conocido en internet]	No	Recuento	43	3	46
			% del total	69,4%	4,8%	74,2%
		Sí	Recuento	12	4	16
			% del total	19,4%	6,5%	25,8%
	Total		Recuento	55	7	62
			% del total	88,7%	11,3%	100,0%
Total	PRETEST De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con personas que he conocido en internet]	No	Recuento	70	6	76
			% del total	65,4%	5,6%	71,0%
		Sí	Recuento	17	14	31
			% del total	15,9%	13,1%	29,0%

	Total	Recuento	87	20	107
		% del total	81,3%	18,7%	100,0%

Tabla 125 Prueba chi-cuadrado predisposición a compartir personas conocidas en internet

POSTEST		Valor	Sig. exacta (bilateral)
Colegio Control	Prueba de McNemar		,727[a]
	N de casos válidos	45	
Colegio Experimental	Prueba de McNemar		,035[a]
	N de casos válidos	62	
Total	Prueba de McNemar		,035[a]
	N de casos válidos	107	

a. Utilizada la distribución binomial

Según los resultados del test de McNemar se aprecian diferencias significativas en los resultados del pretest y el postest respecto a tener la pregunta 'De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? [Con personas que he conocido en internet]' en la muestra total (p=0,035) y en el grupo experimental (p=0,035). Sin embargo, no se producen cambio en el grupo de control (p=0,727).

En la de **Tabla 124** se puede apreciar que el 75% de los jóvenes que antes de la intervención afirmaron que compartirían una foto o vídeo en el que aparezcan, con personas que han conocido en internet, no lo harían tras la intervención.

Predisposición a compartir información con personas conocidas en internet

Tabla 126 Contingencia predisposición a compartir e-mail con desconocidos

POSTEST				POSTEST Email		Total
				No	Sí	
Colegio Control	PRETEST Email	No	Recuento	33	4	37
			% del total	73,3%	8,9%	82,2%

Colegio Experimental	PRETEST Email	Sí	Recuento	4	4	8
			% del total	8,9%	8,9%	17,8%
		Total	Recuento	37	8	45
			% del total	82,2%	17,8%	100,0%
		No	Recuento	55	3	58
			% del total	88,7%	4,8%	93,5%
		Sí	Recuento	4	0	4
			% del total	6,5%	0,0%	6,5%
		Total	Recuento	59	3	62
			% del total	95,2%	4,8%	100,0%

Tabla 127 Chi-cuadrado predisposición a compartir e-mail con desconocidos

	POSTEST		Valor	Sig. exacta (bilateral)
Colegio Control PRE	Colegio Control POST	Prueba de McNemar		1,000[a]
		N de casos válidos	45	
	Total	Prueba de McNemar		1,000[a]
		N de casos válidos	45	
Colegio Experimental PRE	Colegio Experimental POST	Prueba de McNemar		1,000[a]
		N de casos válidos	62	
	Total	Prueba de McNemar		1,000[a]
		N de casos válidos	62	

a. Utilizada la distribución binomial

Según los resultados del test de McNemar no se aprecian diferencias significativas en los resultados del pretest y el postest del grupo control ni grupo experimental respecto a compartir el e-mail con personas conocidas en internet (p=1,0)

Tabla 128 Contingencia predisposición a compartir información con desconocidos teléfono

POSTEST				POSTEST Número de teléfono		Total
				No	Sí	
Colegio Control	PRETEST Número de teléfono	No	Recuento	33	3	36
			% del total	73,3%	6,7%	80,0%
		Sí	Recuento	5	4	9
			% del total	11,1%	8,9%	20,0%
	Total		Recuento	38	7	45
			% del total	84,4%	15,6%	100,0%
Colegio Experimental	PRETEST Número de teléfono	No	Recuento	54	5	59
			% del total	87,1%	8,1%	95,2%
		Sí	Recuento	2	1	3
			% del total	3,2%	1,6%	4,8%
	Total		Recuento	56	6	62
			% del total	90,3%	9,7%	100,0%

Tabla 129 Chi-cuadrado predisposición a compartir información con desconocidos teléfono

	POSTEST		Valor	Sig. exacta (bilateral)
Colegio Control PRE	Colegio Control POST	Prueba de McNemar		,727[a]
		N de casos válidos	45	
	Total	Prueba de McNemar		,727[a]
		N de casos válidos	45	
Colegio Experimental PRE	Colegio Experimental POST	Prueba de McNemar		,453[a]
		N de casos válidos	62	
	Total	Prueba de McNemar		,453[a]
		N de casos válidos	62	

a. Utilizada la distribución binomial

Según los resultados del test de McNemar no se aprecian diferencias significativas en los resultados del pretest y el postest del grupo control (p=0,727) ni grupo experimental (p=0,453) respecto a compartir el número de teléfono con personas conocidas en internet.

Predisposición uso de la webcam con amigos

Tabla 130 Contingencia predisposición uso de la webcam con amigos

				POSTEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con mis amigos]		Total
				No	Sí	
Colegio Control	PRETEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con mis amigos]	No	Recuento	13	10	23
			% del total	28,9%	22,2%	51,1%
		Sí	Recuento	9	13	22
			% del total	20,0%	28,9%	48,9%
	Total		Recuento	22	23	45
			% del total	48,9%	51,1%	100,0%
Colegio Experimental	PRETEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con mis amigos]	No	Recuento	14	15	29
			% del total	22,6%	24,2%	46,8%
		Sí	Recuento	23	10	33
			% del total	37,1%	16,1%	53,2%
	Total		Recuento	37	25	62
			% del total	59,7%	40,3%	100,0%
Total	PRETEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con mis amigos]	No	Recuento	27	25	52
			% del total	25,2%	23,4%	48,6%
		Sí	Recuento	32	23	55
			% del total	29,9%	21,5%	51,4%
	Total		Recuento	59	48	107
			% del total	55,1%	44,9%	100,0%

Tabla 131 Pruebas de chi-cuadrado predisposición uso de la webcam con amigos

POSTEST		Valor	Sig. exacta (bilateral)
Colegio Control	Prueba de McNemar		1,000[a]
	N de casos válidos	45	
Colegio Experimental	Prueba de McNemar		,256[a]
	N de casos válidos	62	
Total	Prueba de McNemar		,427[a]
	N de casos válidos	107	

a. Utilizada la distribución binomial

Según los resultados del test de McNemar no se aprecian diferencias significativas en los resultados del pretest y el postest respecto a tener la pregunta 'De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con mis amigos]' en la muestra total (p=0,427), ni en el grupo de control (p=1,0) ni en el grupo experimental (p=0,256).

Predisposición uso de la webcam con amigos de mis amigos

Tabla 132 Contingencia predisposición uso de la webcam con amigos de mis amigos

POSTEST				POSTEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con amigos de mis amigos]		Total
				No	Sí	
Colegio Control	PRETEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con amigos de mis amigos]	No	Recuento	34	5	39
			% del total	75,6%	11,1%	86,7%
		Sí	Recuento	3	3	6
			% del total	6,7%	6,7%	13,3%
	Total		Recuento	37	8	45
			% del total	82,2%	17,8%	100,0%
Colegio Experimental	PRETEST De las siguientes 'personas', ¿con quienes utilizarías	No	Recuento	50	6	56
			% del total	80,6%	9,7%	90,3%
		Sí	Recuento	6	0	6

	una webcam? [Con amigos de mis amigos]		% del total	9,7%	0,0%	9,7%
	Total		Recuento	56	6	62
			% del total	90,3%	9,7%	100,0%
Total	PRETEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con amigos de mis amigos]	No	Recuento	84	11	95
			% del total	78,5%	10,3%	88,8%
		Sí	Recuento	9	3	12
			% del total	8,4%	2,8%	11,2%
	Total		Recuento	93	14	107
			% del total	86,9%	13,1%	100,0%

Tabla 133 Pruebas de chi-cuadrado predisposición uso de la webcam con amigos de mis amigos

POSTEST		Valor	Sig. exacta (bilateral)
Colegio Control	Prueba de McNemar		,727[a]
	N de casos válidos	45	
Colegio Experimental	Prueba de McNemar		1,000[a]
	N de casos válidos	62	
Total	Prueba de McNemar		,824[a]
	N de casos válidos	107	

a. Utilizada la distribución binomial

Según los resultados del test de McNemar no se aprecian diferencias significativas en los resultados del pretest y el postest respecto a tener la pregunta 'De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con amigos de mis amigos]' en la muestra total (p=0,824), ni en el grupo de control (p=0,727) ni en el grupo experimental (p=1,0).

Predisposición uso de la webcam con conocidos en internet

Tabla 134 Contingencia predisposición uso de la webcam con conocidos en internet

POSTEST				POSTEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Conocidos en internet]		Total
				No	Sí	
Colegio Control	PRETEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Conocidos en internet]	No	Recuento	45		45
			% del total	100,0%		100,0%
	Total		Recuento	45		45
			% del total	100,0%		100,0%
Colegio Experimental	PRETEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Conocidos en internet]	No	Recuento	55	3	58
			% del total	88,7%	4,8%	93,5%
		Sí	Recuento	4	0	4
			% del total	6,5%	0,0%	6,5%
	Total		Recuento	59	3	62
			% del total	95,2%	4,8%	100,0%
Total	PRETEST De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Conocidos en internet]	No	Recuento	100	3	103
			% del total	93,5%	2,8%	96,3%
		Sí	Recuento	4	0	4
			% del total	3,7%	0,0%	3,7%
	Total		Recuento	104	3	107
			% del total	97,2%	2,8%	100,0%

Tabla 135 Pruebas de chi-cuadrado predisposición uso de la webcam con conocidos en internet

POSTEST		Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)
Colegio Control	N de casos válidos	45			
	Prueba de McNemar-Bowker	.	.	.[b]	

Colegio Experimental	Prueba de McNemar		1,000[a]
	N de casos válidos	62	
Total	Prueba de McNemar		1,000[a]
	N de casos válidos	107	

a. Utilizada la distribución binomial

b. Sólo se efectuará el cálculo para tablas de PxP, donde P debe ser mayor que 1.

No se puede calcular la p de McNemar en el grupo de control porque ninguno compartiría la webcam con personas conocidas en internet. En el caso del grupo experimental si bien hay algunos cambios aunque no son significativos, según la p de McNemar (p=1,0). Hay 3 personas que pasaron del no al sí y 4 y 3 que lo hicieron en sentido contrario, estos cambios pueden deberse al azar. Por tanto, según los resultados del test de McNemar no se aprecian diferencias significativas en los resultados del pretest y el postest respecto a tener la pregunta 'De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con personas conocidas en internet]' en el grupo experimental (p=0,256).

Uso Software de protección en ordenador de casa

Tabla 136 Contingencia uso software de protección en ordenador de casa

	POSTEST			POSTEST ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu ordenador de casa?		Total
				No	Sí	
Colegio Control	PRETEST ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu ordenador de casa?	No	Recuento	6	5	11
			% del total	15,8%	13,2%	28,9%
		Sí	Recuento	4	23	27
			% del total	10,5%	60,5%	71,1%
	Total		Recuento	10	28	38
			% del total	26,3%	73,7%	100,0%
Colegio Experimental	PRETEST ¿Tienes	No	Recuento	0	3	3

	instalado software de protección, como por ejemplo un antivirus, en tu ordenador de casa?		% del total	0,0%	4,9%	4,9%
		Sí	Recuento	1	57	58
			% del total	1,6%	93,4%	95,1%
		Total	Recuento	1	60	61
			% del total	1,6%	98,4%	100,0%
Total	PRETEST ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu ordenador de casa?	No	Recuento	6	8	14
			% del total	6,1%	8,1%	14,1%
		Sí	Recuento	5	80	85
			% del total	5,1%	80,8%	85,9%
		Total	Recuento	11	88	99
			% del total	11,1%	88,9%	100,0%

Tabla 137 Pruebas de chi-cuadrado uso software de protección en ordenador de casa

POSTEST		Valor	Sig. exacta (bilateral)
Colegio Control POST	Prueba de McNemar		1,000[a]
	N de casos válidos	38	
Colegio Experimental POST	Prueba de McNemar		,625[a]
	N de casos válidos	61	
Total	Prueba de McNemar		,581[a]
	N de casos válidos	99	

a. Utilizada la distribución binomial

Según los resultados del test de McNemar no se aprecian diferencias significativas en los resultados del pretest y el postest respecto a tener la pregunta '¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu ordenador de casa?' en la muestra total (p=0,581), ni en el grupo de control (p=1,0) ni en el grupo experimental (p=0,625).

Uso software de protección en el Smartphone

Tabla 138 Contingencia uso software de protección en Smartphone

POSTEST				POSTEST ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu Smartphone?		Total
				No	Sí	
Colegio Control	PRETEST ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu Smartphone?	No	Recuento	12	3	15
			% del total	42,9%	10,7%	53,6%
		Sí	Recuento	3	10	13
			% del total	10,7%	35,7%	46,4%
	Total		Recuento	15	13	28
			% del total	53,6%	46,4%	100,0%
Colegio Experimental	PRETEST ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu Smartphone?	No	Recuento	6	14	20
			% del total	10,9%	25,5%	36,4%
		Sí	Recuento	7	28	35
			% del total	12,7%	50,9%	63,6%
	Total		Recuento	13	42	55
			% del total	23,6%	76,4%	100,0%
Total	PRETEST ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu Smartphone?	No	Recuento	18	17	35
			% del total	21,7%	20,5%	42,2%
		Sí	Recuento	10	38	48
			% del total	12,0%	45,8%	57,8%
	Total		Recuento	28	55	83
			% del total	33,7%	66,3%	100,0%

Tabla 139 Pruebas de chi-cuadrado uso software de protección en Smartphone

POSTEST		Valor	Sig. exacta (bilateral)
Colegio Control	Prueba de McNemar		1,000[a]
	N de casos válidos	28	
Colegio Experimental	Prueba de McNemar		,189[a]
	N de casos válidos	55	
Total	Prueba de McNemar		,248[a]
	N de casos válidos	83	

a. Utilizada la distribución binomial

Según los resultados del test de McNemar no se aprecian diferencias significativas en los resultados del pretest y el postest respecto a tener la pregunta '¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu Smartphone?' en la muestra total (p=0,248), ni en el grupo de control (p=1,0) ni en el grupo experimental (p=0,189).

Análisis de las variables de la escala Likert

Dado que las variables analizadas no tienen distribución normal, para poder analizar los resultados obtenidos en el tiempo a través del pretest y el postest, de las variables que utilizar la escala Likert, empleamos la prueba de Wilcoxon para dos muestras relacionadas.

En la **Tabla 140** *Estadísticos descriptivos escala Likert*nos muestra los estadísticos descriptivos de cada variable y sus respectivos tamaños muestrales. La tabla está dividida en dos grupos: control y experimental, y luego entre resultados pretest y postest.

Tabla 140 Estadísticos descriptivos escala Likert

	Variables	PRETEST				POSTEST			
		N	Media	Desviación típica	Mediana	N	Media	Desviación típica	Mediana
Colegio Control	Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	45	4,36	1,151	5	45	4,422	1,03328	5

Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	45	1,93	1,388	1	45	2,044	1,46094	1
Sólo entro en páginas web recomendadas para mi edad	45	2,76	1,479	3	45	2,822	1,36995	3
Los chats públicos son páginas seguras donde nadie puede hacerme nada	45	2,16	1,278	2	45	2,022	1,21522	2
No pasa nada por descargar música o aplicaciones "pirateadas"	45	3,02	1,357	3	45	3,022	1,35661	3
Si conozco a alguien simpático/a jugando en red, le agregaría como 'amigo/a' en mi red social	45	2,44	1,486	2	45	2,622	1,4968	2
Si una página web me pide el número de teléfono, se lo doy	45	1,73	1,095	1	45	1,622	1,02888	1
Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	45	1,78	1,295	1	45	1,733	1,19469	1

	Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	45	2,18	1,353	2	45	2,244	1,44844	2
	Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	62	4,63	0,752	5	62	4,758	0,5919	5
	Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	62	1,61	0,964	1	62	1,452	0,86228	1
Colegio Experimental	Sólo entro en páginas web recomendadas para mi edad	62	3,37	1,462	3,5	62	3,242	1,43362	3
	Los chats públicos son páginas seguras donde nadie puede hacerme nada	62	2,48	1,277	2	62	1,984	1,07874	2
	No pasa nada por descargar música o aplicaciones “pirateadas”	62	3,05	1,234	3	62	2,548	1,27623	3
	Si conozco a alguien simpático/a jugando en red, le agregaría como ‘amigo/a’ en mi red social	62	2,29	1,193	2	62	1,984	1,1234	2

Si una página web me pide el número de teléfono, se lo doy	62	1,71	1,179	1	62	1,516	0,91869	1
Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	62	1,61	1,03	1	62	1,597	1,07825	1
Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	62	1,76	1,169	1	62	1,516	0,91869	1

Resultados de las pruebas de Wilcoxon para muestras relacionadas:

La **Tabla 141** muestra, por separado, las diferencias entre el pretest y postest del grupo de control y del grupo experimental. El estadístico Z (correspondiente a Wilcoxon) y su respectiva p obtiene las diferencias, si las hubiese, entre los resultados del pretest y postest.

Tabla 141 Estadísticos de contraste impacto variables escala Likert

	POSTEST			
	Colegio Control POST		Colegio Experimental POST	
	Z	Sig. asintót. (bilateral)	Z	Sig. asintót. (bilateral)
Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	-,217[c]	,828	-1,208[c]	,227
Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	-,547[c]	,584	-,870	,384
Sólo entro en páginas web recomendadas para mi edad	-,321[c]	,748	-,489	,625
Los chats públicos son páginas seguras donde nadie puede hacerme nada	-,791	,429	-2,248	,025
No pasa nada por descargar música o aplicaciones "pirateadas"	-,066[c]	,947	-2,117	,034
Si conozco a alguien simpático/a jugando en red, le agregaría como 'amigo/a' en mi red social	-,813[c]	,416	-1,271	,204
Si una página web me pide el número de teléfono, se lo doy	-,711	,477	-1,024	,306
Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	-,177	,860	-,012	,990
Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	-,303[c]	,762	-1,315	,188

a. Prueba de los rangos con signo de Wilcoxon

c. Basado en los rangos negativos.

Los resultados indican que no hay diferencias significativas en los resultados pretest y postest del grupo de control respecto a su valoración en las variables incluidas en las pruebas Wilcoxon para muestras relacionadas.

Sin embargo, podemos apreciar que en el grupo experimental se han hallado resultados que indican que existen diferencias significativas en los resultados pretest y postest, que son las siguientes:

- Respecto a la pregunta 'Los chats públicos son páginas seguras donde nadie puede hacerme nada' encontramos que la valoración del postest obtiene diferencias signicativas respecto a los resultados del pretest (Z=-2,248, p=0,025).
- Respecto a la pregunta 'No pasa nada por descargar música o aplicaciones "pirateadas" se obtienen resultados significativos respecto a la variación entre el pretest y postest (Z=-2,117, p=0,034)

3.2. Otros análisis relevantes del postest

A continuación, se exponen los resultados hallados en las variables incluidas únicamente en el postest, con el objetivo de conocer determinadas acciones realizadas por los jóvenes tras la intervención en beneficio de la seguridad con la que hacen uso de las TIC.

Fotos o vídeos eliminados tras la intervención en las RRSS

Se ha incluido ésta pregunta con el objetivo de conocer el efecto inmediato que ha tenido la intervención sobre la información audiovisual de las redes sociales de los jóvenes.

Tabla 142 Fotos o vídeos eliminados tras la intervención en las RRSS

POSTEST		Frecuencia	Porcentaje
Colegio Control	No tengo RRSS	5	11,1
	Ninguna	24	53,3
	Pocas	8	17,8
	Algunas	5	11,1
	Bastantes	2	4,4
	Muchas	1	2,2
	Total	45	100,0
Colegio Experimental	No tengo RRSS	5	8,1
	Ninguna	19	30,6
	Pocas	20	32,3
	Algunas	9	14,5
	Bastantes	2	3,2
	Muchas	7	11,3
	Total	62	100,0

En la **Tabla 142** se puede apreciar que el 61,3% de los participantes del grupo experimental han eliminado fotos o vídeos tras la intervención. Por su parte, en el grupo de control el 35,6% de los participantes también realizaron la acción.

Tabla 143 Prueba Monte Carlo fotos eliminadas tras la intervención

	Valor	gl	Sig. asintótica (bilateral)	Sig. de Monte Carlo (bilateral)		
				Sig.	Intervalo de confianza al 99%	
					Límite inferior	Límite superior
Chi-cuadrado de Pearson	8,891[a]	5	,114	,110	,102	,118

Razón de verosimilitudes	9,404	5	,094	,127	,119	,136
Estadístico exacto de Fisher	8,838			,103	,095	,110
Asociación lineal por lineal	4,918[c]	1	,027	,030	,026	,035
N de casos válidos	107					

a. 5 casillas (41,7%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 1,68.
c. El estadístico tipificado es 2,218.

Se puede apreciar que las pruebas realizadas sobre la variable fotos o vídeos eliminados tras la intervención muestra ser no significativa al obtener en la prueba de Monte Carlo que p=0,110.

Revisión de la configuración de seguridad y privacidad de las RRSS

A continuación, podemos observar los jóvenes que han revisado o modificado la configuración de seguridad y privacidad de sus redes sociales tras la intervención.

Tabla 144 Revisión de la configuración de seguridad y privacidad de las RRSS

			Colegio Control	Colegio Experimental	Total
En el último mes, ¿has revisado o modificado la configuración de seguridad y privacidad de tu red social?	No	Recuento	27	27	54
		%	67,5%	47,4%	55,7%
	Sí	Recuento	13	30	43
		%	32,5%	52,6%	44,3%
Total		Recuento	40	57	97
		%	100,0%	100,0%	100,0%

Tabla 145 Prueba chi-cuadrado revisión configuración tras la intervención

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	3,860[a]	1	,049		
Corrección por continuidad[b]	3,087	1	,079		
Razón de verosimilitudes	3,913	1	,048		
Estadístico exacto de Fisher				,063	,039
Asociación lineal por lineal	3,820	1	,051		
N de casos válidos	97				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 17,73.

b. Calculado sólo para una tabla de 2x2.

En la **Tabla 144** se observa que tras la intervención el 52,6% de los jóvenes que forman parte del grupo experimental, revisaron o modificaron la configuración de seguridad y privacidad de sus redes sociales, mientras que en el grupo de control lo hicieron el 32,5%. Además, en la **Tabla 145** se obtiene que los resultados han mostrado ser significativos respecto a la variable Información previa sobre hábitos seguros y responsables (Chi-cuadrado: 3,860; gl = 1; p=0,49).

Relación entre configuración de la seguridad y modificación de la configuración de seguridad

A continuación, analizamos si la percepción de los jóvenes sobre la necesidad de configurar ellos mismos la seguridad y privacidad de sus redes sociales, está relacionado con la acción de haberla modificado o revisado tras la intervención.

Tabla 146 Contingencia asociación variables configuración seguridad

Postest			En el último mes, ¿has revisado o modificado la configuración de seguridad y privacidad de tu red social?		Total
			No	Sí	
¿Consideras necesario configurar tú mismo/a la seguridad y privacidad de tus redes sociales?	No	Recuento	10	0	10
		Porcentaje	100,0%	0,0%	100,0%
	Sí	Recuento	16	30	46
		Porcentaje	34,8%	65,2%	100,0%
Total		Recuento	26	30	56
		Porcentaje	46,4%	53,6%	100,0%

Tabla 147 Prueba chi-cuadrado asociación variables configuración seguridad

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	14,047[a]	1	,000		
Corrección por continuidad[b]	11,547	1	,001		
Razón de verosimilitudes	17,906	1	,000		
Estadístico exacto de Fisher				,000	,000
Asociación lineal por lineal	13,796	1	,000		
N de casos válidos	56				

a. 1 casillas (25,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 4,64.

b. Calculado sólo para una tabla de 2x2.

En la **Tabla 146** podemos observar que el 65,2% de los jóvenes que consideran necesario ser ellos mismos quienes revisen y modifiquen la seguridad y privacidad de sus redes sociales, la han revisado tras la intervención. Además, se confirma la asociación entre las variables (Chi-cuadrado: 14,047; gl = 1; p< 0,001), siendo la significación obtenida en el método Fisher p<0,001.

Relación entre necesidad software seguridad e instalación

En éste apartado analizamos la asociación entre las variables relacionadas con el uso de software de protección en los dispositivos de conexión a internet.

Tabla 148 Contingencia relación necesidad antivirus instalación

POSTEST ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu Smartphone?	Media	Mediana	Rango	Mínimo	Máximo	Desv.típ.	N
No	4,3226	5,0000	4,00	1,00	5,00	1,04521	31
Sí	4,7742	5,0000	2,00	3,00	5,00	,52540	62
Total	4,6237	5,0000	4,00	1,00	5,00	,76491	93

Tabla 149 Prueba U de Mann-Whiney relación software de seguridad e instalación

	POSTEST Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone
U de Mann-Whitney	741,500
W de Wilcoxon	1237,500
Z	-2,370
Sig. asintót. (bilateral)	,018

a. Variable de agrupación: POSTEST ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu Smartphone?

La prueba U de Mann-Whitney (véase **Tabla 149**) indica que existe relación entre las variables analizadas (U de M-W: 741,5; Z=-2,37; p=0,018).

3.3. Análisis de la influencia de la variable “género” en el postest

A continuación, vamos a analizar la significación del género como variable independiente en el postest. Para ello, al igual que anteriormente, utilizaremos la prueba

de chi-cuadrado que nos permite conocer la relación del género con los hábitos que son medidos en el cuestionario.

En las tablas de contingencia podremos observar la relación del género con todas las diferentes preguntas del cuestionario postest. Hay que tener en cuenta que no se están analizando estadísticamente las diferencias entre grupo experimental y de control, sólo se comparan los resultados obtenidos en cada uno de los grupos que forman parte de la investigación.

Únicamente, se exponen las tablas que contengan resultados significativos hallados del cruce de la variable género con el resto de variables del estudio.

Comentario inadecuado

Tabla 150 Contingencia percepción comentarios inadecuados en RRSS

	POSTEST			POSTEST		Total
				Hombre	Mujer	
Colegio Control	¿Alguno de los comentarios, que tienes en tus redes sociales, podría parecerles inadecuado a tus padres si lo vieran?	No	Recuento	14	13	27
			% género	77,8%	59,1%	67,5%
		Sí	Recuento	4	9	13
			% género	22,2%	40,9%	32,5%
	Total		Recuento	18	22	40
			% género	100,0%	100,0%	100,0%
Colegio Experimental	¿Alguno de los comentarios, que tienes en tus redes sociales, podría parecerles inadecuado a tus padres si lo vieran?	No	Recuento	17	28	45
			% género	65,4%	90,3%	78,9%
		Sí	Recuento	9	3	12
			% género	34,6%	9,7%	21,1%
	Total		Recuento	26	31	57
			% género	100,0%	100,0%	100,0%
Total	¿Alguno de los comentarios, que tienes en	No	Recuento	31	41	72
			% género	70,5%	77,4%	74,2%

	tus redes sociales, podría parecerles inadecuado a tus padres si lo vieran?	Sí	Recuento	13	12	25
			% género	29,5%	22,6%	25,8%
	Total		Recuento	44	53	97
			% género	100,0%	100,0%	100,0%

Tabla 151 Chi-cuadrado percepción comentarios inadecuados en RRSS

POSTEST		Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Colegio Control	Chi-cuadrado de Pearson	1,576[c]	1	,209		
	Corrección por continuidad[b]	,839	1	,360		
	Razón de verosimilitudes	1,610	1	,205		
	Estadístico exacto de Fisher				,312	,180
	Asociación lineal por lineal	1,536	1	,215		
	N de casos válidos	40				
Colegio Experimental	Chi-cuadrado de Pearson	5,291[d]	1	,021		
	Corrección por continuidad[b]	3,897	1	,048		
	Razón de verosimilitudes	5,417	1	,020		
	Estadístico exacto de Fisher				,027	,024
	Asociación lineal por lineal	5,198	1	,023		
	N de casos válidos	57				
Total	Chi-cuadrado de Pearson	,599[a]	1	,439		
	Corrección por continuidad[b]	,292	1	,589		
	Razón de verosimilitudes	,597	1	,440		
	Estadístico exacto de Fisher				,490	,294
	Asociación lineal por lineal	,593	1	,441		
	N de casos válidos	97				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 11,34.

b. Calculado sólo para una tabla de 2x2.

c. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 5,85.

d. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 5,47.

La percepción de los jóvenes sobre la calidad de sus comentarios en redes sociales obtiene resultados desiguales entre los grupos. Por un lado, el grupo de control y el total de la muestra no hayan diferencias entre los chicos y las chicas, hayando (Chi-

cuadrado: 1,576; gl: 1; p=0,209) y (Chi-cuadrado: 0,599; gl: 1; p=0,439) respectivamente. Sin embargo, no ocurre lo mismo con el grupo experimental que haya diferencias significativas entre ambos géneros (Chi-cuadrado: 5,291; gl: 1; p=0,021) debido a que la proporción de mujeres que dicen no tener comentarios inadecuados en sus redes sociales, 90,3%, es superior al de los hombres, 65,4%.

Predisposición Uso de la webcam con amigos

Tabla 152 Contingencia predisposición Uso de la webcam con amigos

	POSTEST			POSTEST		Total
				Hombre	Mujer	
Colegio Control	De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con mis amigos]	No	Recuento	11	11	22
			% género	52,4%	45,8%	48,9%
		Sí	Recuento	10	13	23
			% género	47,6%	54,2%	51,1%
	Total		Recuento	21	24	45
			% género	100,0%	100,0%	100,0%
Colegio Experimental	De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con mis amigos]	No	Recuento	19	18	37
			% género	65,5%	54,5%	59,7%
		Sí	Recuento	10	15	25
			% género	34,5%	45,5%	40,3%
	Total		Recuento	29	33	62
			% género	100,0%	100,0%	100,0%
Total	De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con mis amigos]	No	Recuento	30	29	59
			% género	60,0%	50,9%	55,1%
		Sí	Recuento	20	28	48
			% género	40,0%	49,1%	44,9%
	Total		Recuento	50	57	107
			% género	100,0%	100,0%	100,0%

Tabla 153 Chi-cuadrado predisposición Uso de la webcam con amigos

POSTEST		Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Colegio Control POST	**Chi-cuadrado de Pearson**	**,192[c]**	**1**	**,661**		
	Corrección por continuidad[b]	,019	1	,889		
	Razón de verosimilitudes	,192	1	,661		
	Estadístico exacto de Fisher				,768	,445
	Asociación lineal por lineal	,188	1	,665		
	N de casos válidos	45				
Colegio Experimental POST	Chi-cuadrado de Pearson	**,772[d]**	**1**	**,380**		
	Corrección por continuidad[b]	,384	1	,536		
	Razón de verosimilitudes	,776	1	,379		
	Estadístico exacto de Fisher				,443	,268
	Asociación lineal por lineal	,760	1	,383		
	N de casos válidos	62				
Total	Chi-cuadrado de Pearson	**,896[a]**	**1**	**,344**		
	Corrección por continuidad[b]	,565	1	,452		
	Razón de verosimilitudes	,898	1	,343		
	Estadístico exacto de Fisher				,436	,226
	Asociación lineal por lineal	,888	1	,346		
	N de casos válidos	107				

a. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 22,43.

b. Calculado sólo para una tabla de 2x2.

c. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 10,27.

d. 0 casillas (,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 11,69.

Las pruebas de Chi-cuadrado nos muestran que no hay relación entre género y la pregunta De las siguientes 'personas', ¿con quienes utilizarías una webcam? [Con mis amigos]. En el grupo de control se obtiene (Chi-cuadrado: 0,192; gl: 1; p=0,661) y en el grupo experimental (Chi-cuadrado: 0,772; gl: 1; p=0,380). Del mismo modo, el total de la muestra no deja dudas sobre la no significación de la variable género en la pregunta planteada (chi-cuadrado: 0,896; gl: 1, p=0,334).

Variables que utilizan escala de Likert

Primero analizo los resultados del grupo de control, para ver si el género influye en las variables que utilizan una escala Likert.

Tabla 154 Estadísticos descriptivos variables escala Likert en el grupo de control

Género		Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	Sólo entro en páginas web recomendadas para mi edad	Los chats públicos son páginas seguras donde nadie puede hacerme nada	No pasa nada por descargar música o aplicaciones "pirateadas"	Si conozco a alguien simpático/a jugando en red, le agregaría como 'amigo/a' en mi red social	Si una página web me pide el número de teléfono, se lo doy	Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona
Hombre	Media	4,4286	1,9524	2,7143	1,6190	2,9524	2,4762	1,8095	1,7619	2,7619
	Mediana	5,0000	1,0000	3,0000	1,0000	3,0000	2,0000	1,0000	1,0000	3,0000
	N	21	21	21	21	21	21	21	21	21
	Desv. típ.	1,24786	1,53219	1,48805	,86465	1,35927	1,40068	1,24976	1,13599	1,44585
Mujer	Media	4,4167	2,1250	2,9167	2,3750	3,0833	2,7500	1,4583	1,7083	**1,7917**
	Mediana	5,0000	1,5000	3,0000	2,0000	3,0000	2,5000	1,0000	1,0000	**1,0000**
	N	24	24	24	24	24	24	24	24	24
	Desv. típ.	,82970	1,42379	1,28255	1,37722	1,38051	1,59483	,77903	1,26763	1,31807
Total	Media	4,4222	2,0444	2,8222	2,0222	3,0222	2,6222	1,6222	1,7333	2,2444
	Mediana	5,0000	1,0000	3,0000	2,0000	3,0000	2,0000	1,0000	1,0000	2,0000
	N	45	45	45	45	45	45	45	45	45
	Desv. típ.	1,03328	1,46094	1,36995	1,21522	1,35661	1,49680	1,02888	1,19469	1,44844

a. **POSTEST = Colegio Control**

Aquí está la prueba U de Mann-Whitney para ver si hay diferencias entre hombres y mujeres dentro del grupo de control.

Tabla 155 U de Mann-Whitney variables escala Likert grupo de control

	U de Mann-Whitney	W de Wilcoxon	Z	Sig. asintót. (bilateral)
Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	223,500	523,500	-,793	,428
Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	222,000	453,000	-,762	,446
Sólo entro en páginas web recomendadas para mi edad	233,000	464,000	-,447	,655
Los chats públicos son páginas seguras donde nadie puede hacerme nada	**173,500**	404,500	**-1,904**	,057
No pasa nada por descargar música o aplicaciones "pirateadas"	238,000	469,000	-,328	,743
Si conozco a alguien simpático/a jugando en red, le agregaría como 'amigo/a' en mi red social	229,500	460,500	-,527	,598
Si una página web me pide el número de teléfono, se lo doy	222,000	522,000	-,816	,414
Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	240,500	540,500	-,307	,759
Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	**152,500**	452,500	**-2,422**	,015

a. POSTEST Colegio Control

b. Variable de agrupación: POSTEST género

El análisis de las variables que usan la escala Likert, nos muestran que tan sólo existe relación significativa con el género, es decir, que los resultados son significativos entre hombres y mujeres respecto a la afirmación: Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona. En la tabla de contingencia podemos ver que los hombres tienen puntuaciones más altas (media: 2,76, mediana: 3) que las mujeres (media: 1,79, mediana: 1). Esta diferencia es estadísticamente significativa (U de M-W:152,500; Z=-2,422; p=0,015).

Además, se aprecia que la relación entre hombres y mujeres respecto a la percepción de seguridad en los chats públicos está claramente diferenciada, estando cerca de ser significativa. Síntoma que nos proporciona la hipótesis que en grupos más grandes se convierta en significativa, (U de M-W:173,5; Z=-1,904; p=0,057).

A continuación, se muestran los resultados obtenidos en el grupo experimental.

Tabla 156 Estadísticos descriptivos variables escala Likert en el grupo de experimental

Género		Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	Sólo entro en páginas web recomendadas para mi edad	Los chats públicos son páginas seguras donde nadie puede hacerme nada	No pasa nada por descargar música o aplicaciones “pirateadas”	Si conozco a alguien simpático/a jugando en red, le agregaría como ‘amigo/a’ en mi red social	Si una página web me pide el número de teléfono, se lo doy	Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona
Hombre	Media	4,6897	1,3448	2,7241	1,9655	2,7241	2,0345	1,5172	1,7241	1,5172

Mujer	Mediana	5,0000	1,0000	3,0000	2,0000	3,0000	1,0000	1,0000	1,0000	1,0000
	N	29	29	29	29	29	29	29	29	29
	Desv. típ.	,71231	,61388	1,38607	1,08505	1,41160	1,26725	,98636	1,22172	,94946
	Media	4,8182	1,5455	3,6970	2,0000	2,3939	1,9394	1,5152	1,4848	1,5152
	Mediana	5,0000	1,0000	4,0000	2,0000	2,0000	2,0000	1,0000	1,0000	1,0000
	N	33	33	33	33	33	33	33	33	33
	Desv. típ.	,46466	1,03353	1,33428	1,08972	1,14399	,99810	,87039	,93946	,90558
Total	Media	4,7581	1,4516	3,2419	1,9839	2,5484	1,9839	1,5161	1,5968	1,5161
	Mediana	5,0000	1,0000	3,0000	2,0000	3,0000	2,0000	1,0000	1,0000	1,0000
	N	62	62	62	62	62	62	62	62	62
	Desv. típ.	,59190	,86228	1,43362	1,07874	1,27623	1,12340	,91869	1,07825	,91869

a. POSTEST Colegio Experimental POST

Los resultados de la prueba U de Mann-Whitney para determinar si hay diferencias en las respuestas de hombres y mujeres son los siguientes:

Tabla 157 U de Mann-Whitney variables escala Likert grupo experimental

	Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	Sólo entro en páginas web recomendadas para mi edad	Los chats públicos son páginas seguras donde nadie puede hacerme nada	No pasa nada por descargar música o aplicaciones “pirateadas”	Si conozco a alguien simpático/a jugando en red, le agregaría como ‘amigo/a’ en mi red social	Si una página web me pide el número de teléfono, se lo doy	Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona

U de Mann-Whitney	449,500	471,500	**293,000**	469,500	420,500	477,000	468,500	439,000	478,000
W de Wilcoxon	884,500	906,500	728,000	904,500	981,500	912,000	903,500	1000,000	1039,000
Z	-,616	-,129	**-2,679**	-,135	-,844	-,023	-,176	-,710	-,009
Sig. asintót. (bilateral)	,538	,898	**,007**	,893	,399	,982	,860	,478	,993

a. POSTEST Colegio Experimental POST

b. Variable de agrupación: POSTEST Género

El análisis de las variables que usan escala Likert, en el grupo experimental, nos muestran que de las variables analizadas existe relación significativa con el género, es decir, que los resultados son significativos entre hombres y mujeres, respecto a la afirmación 'Sólo entro en páginas web recomendadas para mi edad'. En la tabla de contingencia podemos ver que los hombres tienen puntuaciones más bajas (media: 2,72, mediana: 3) que las mujeres (media: 3,7, mediana: 4). Esta diferencia es estadísticamente significativa (U de M-W:293,0; Z=-2,679; p=0,007).

Tabla 158 Estadísticos descriptivos variables escala Likert en el total de la muestra

Género		Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	Sólo entro en páginas web recomendadas para mi edad	Los chats públicos son páginas seguras donde nadie puede hacerme nada	No pasa nada por descargar música o aplicaciones "pirateadas"	Si conozco a alguien simpático/a jugando en red, le agregaría como 'amigo/a' en mi red social	Si una página web me pide el número de teléfono, se lo doy	Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona
Hombre	Media	4,5800	1,6000	2,7200	1,8200	2,8200	2,2200	1,6400	1,7400	2,0400
	Mediana	5,0000	1,0000	3,0000	2,0000	3,0000	2,0000	1,0000	1,0000	1,0000
	N	50	50	50	50	50	50	50	50	50

Mujer	Desv. típ.	,97080	1,12486	1,41479	1,00387	1,38048	1,32926	1,10213	1,17473	1,32419
	Media	4,6491	1,7895	3,3684	2,1579	2,6842	2,2807	1,4912	1,5789	1,6316
	Mediana	5,0000	1,0000	3,0000	2,0000	3,0000	2,0000	1,0000	1,0000	1,0000
	N	57	57	57	57	57	57	57	57	57
Total	Desv. típ.	,66792	1,23544	1,35793	1,22167	1,28394	1,33302	,82641	1,08475	1,09596
	Media	4,6168	1,7009	3,0654	2,0000	2,7477	2,2523	1,5607	1,6542	1,8224
	Mediana	5,0000	1,0000	3,0000	2,0000	3,0000	2,0000	1,0000	1,0000	1,0000
	N	107	107	107	107	107	107	107	107	107
	Desv. típ.	,82009	1,18334	1,41602	1,13270	1,32532	1,32532	,96326	1,12521	1,21944

Los estadísticos de contraste para esta última tabla son:

Tabla 159 U de Mann-Whitney variables escala Likert total de la muestra

	Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	Sólo entro en páginas web recomendadas para mi edad	Los chats públicos son páginas seguras donde nadie puede hacerme nada	No pasa nada por descargar música o aplicaciones “pirateadas”	Si conozco a alguien simpático/a jugando en red, le agregaría como ‘amigo/a’ en mi red social	Si una página web me pide el número de teléfono, se lo doy	Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona
U de Mann-Whitney	1399,500	1326,500	**1065,500**	1218,000	1351,500	1380,500	1371,500	1329,000	1178,000
W de Wilcoxon	3052,500	2601,500	2340,500	2493,000	3004,500	2655,500	3024,500	2982,000	2831,000
Z	-,215	-,739	**-2,300**	-1,374	-,472	-,291	-,409	-,734	-1,782
Sig. asintót. (bilateral)	,830	,460	**,021**	,170	,637	,771	,682	,463	,075

a. Variable de agrupación: POSTEST Género

Si incluimos en el análisis a toda la muestra, del mismo modo que en los resultados que se han obtenido en el grupo experimental, se observan diferencias significativas entre hombres y mujeres respecto a la afirmación 'Solo entro en páginas web recomendadas para mi edad'.

En la **Tabla 158** podemos ver que los hombres tienen puntuaciones más bajas (media: 2,72, mediana: 3) que las mujeres (media: 3,37, mediana: 3). Esta diferencia es estadísticamente significativa (U de M-W:1065,500; Z=-2,300; p=0,021).

3.4. Síntesis de los resultados pretest-postest

En éste apartado expondremos los resultados considerados más relevantes en el análisis de la eficacia de la intervención.

A través, del análisis de los resultados obtenidos en el pretest y postest daremos respuesta a las hipótesis 3 e hipótesis 4. Para ello, se han utilizado pruebas estadísticas que nos permiten analizar los resultados obtenidos en distintos momentos. Como hemos podido apreciar, en nuestro caso, se ha utilizado mayoritariamente McNemar.

3.4.1. Análisis de las variables del estudio

A continuación, analizaremos las conclusiones de los hábitos que han experimentado cambios relevantes en el estudio.

- Configurar seguridad y privacidad:

Los jóvenes deben responsabilizarse de configurar la configuración y privacidad de sus redes sociales atendiendo a sus intereses y seguridad. Por éste motivo, en la intervención se analizaron los efectos de seleccionar cada una de las opciones de configuración de seguridad y privacidad que ofrecen las principales redes sociales.

En la **Tabla 118** se puede apreciar que en el 84,7% de los jóvenes del grupo experimental, tras la intervención, consideran necesario configurar ellos mismos la seguridad y privacidad de sus redes sociales, mientras que el pretest obtuvo un 42,4%. Además, es significativo, que el 85,3% de los jóvenes que antes de la intervención no consideraban necesario configurar ellos mismos la seguridad y privacidad de sus redes sociales, tras la intervención si lo consideran necesario. Ver **Tabla 118**.

Según los resultados del test de McNemar se aprecian diferencias significativas en los resultados del pretest y el postest respecto a la pregunta '¿Consideras necesario configurar tú mismo/a la seguridad y privacidad de tus redes sociales?' en la muestra total ($p=0,002$) y en el grupo experimental ($p<0,001$). Por su parte, no se producen cambios en el grupo de control ($p=1,0$). Ver **Tabla 119**

- Compartir información audio-visual

Las aplicaciones de redes sociales permiten a los usuarios compartir comentarios, fotos, imágenes, vídeos, etc. A lo largo de la investigación se ha podido apreciar que los jóvenes comparten información a través de sus redes sociales ya sea a través de comentarios u opiniones, o de forma visual mediante fotografías o vídeos. En la intervención se incidió en las consecuencias de compartir información personal a

través de aplicaciones web como las redes sociales y, de este modo, que los jóvenes se responsabilicen de sus decisiones y reflexionen sobre los beneficios y perjuicios de compartir información audiovisual. En éste sentido, se han obtenido las siguientes conclusiones del análisis de los resultados obtenidos en las pruebas realizadas de la variación de resultados entre el pretest y el postest.

En la tabla de contingencia de 'Compartir fotos o vídeos con personas conocidas en internet' (véase **Tabla 124**) se aprecia que antes de la intervención el 25,8% respondían afirmativamente a la pregunta, sin embargo, en el postest tan sólo lo hacen el 11,3%. Esto significa que el 75% de los jóvenes, del grupo experimental, que mostraron su predisposición a compartir información audiovisual con personas conocidas en internet, han cambiado su respuesta tras la intervención. Además, la prueba de McNemar obtiene que las diferencias son significativas en el grupo experimental (p=0,035) y en el total de la muestra (p=0,035), al contrario de lo que ocurre en el grupo control (p=0'727). Sin embargo, los resultados obtenidos sobre compartir información audiovisual con amigos y amigos de mis amigos, obtiene cambios que no resultan significativos según las pruebas realizadas con el test McNemar donde p=0,625 en el caso de compartirlas con 'amigos' y p=0,597 para compartirlas con 'amigos de mis amigos'.

- Webcam

Los resultados obtenidos en la evolución de la exposición al riesgo en el uso de la webcam, con personas conocidas en internet, pese a resultar no significativos y, por lo tanto, no pueden ser atribuidos a la intervención, nos ofrecen información que debe ser mencionada.

En el pretest los participantes del grupo experimental y grupo de control muestran su rechazo a usar la webcam con personas que han conocido en internet, en el 100% y 93,5% de los casos respectivamente. En el grupo experimental tan sólo 4 personas muestran su predisposición a utilizarla con personas que han conocido a través de la red. Tras la intervención, en el grupo experimental se incremente el rechazo, ascendiendo al 95,2%, aunque, los resultados no pueden atribuirse a la intervención como muestran los resultados de la p de McNemar (p=1,0). No obstante, pese a obtenerse resultados satisfactorios, debido a los riesgos derivados del uso de la webcam con personas conocidas en internet, es necesario seguir incidiendo en la presencia del riesgo hasta que los resultados muestren que ningún joven se exponga a los riesgos que derivan de él.

- Software de protección

El uso de software de protección protege los dispositivos de conexión a internet de accesos indeseados a la información del usuario, convirtiéndose en una modalidad de robo de información que en ocasiones trasciende en chantajes y extorsión. En éste sentido, se ha pretendido que los jóvenes conozcan las formas de robo de información y ataque cibernético, así como las recomendaciones para hacerles frente, como es el uso de software de protección.

Los resultados muestran que antes de la intervención el 36,4% de los jóvenes no disponen de software de protección instalado en sus Smartphones, encontrándose una evolución positiva tras la intervención al disminuir hasta el 23,6%. No obstante, la p de McNemar encuentra no significativo el resultado (p=0,189) por lo que los resultados pueden deberse a motivos ajenos a la intervención.

- Percepción de seguridad en chats públicos

En la intervención se procuró valorar con los jóvenes los riesgos que existen en los chats públicos donde se facilita el contacto con personas desconocidas sin necesidad, si quiera, de autenticarse. Por éste motivo se incluyó la pregunta en los cuestionarios y así poder conocer la percepción de los riesgos que existen en los chats públicos y por ende, del contacto con personas desconocidas.

Los resultados hallados muestran que se han encontrado diferencias significativas de los resultados obtenidos entre el pretest y el postest (Z=-2,248, p=0,025) (véase **Tabla 141**). La media obtenida en entre el pretest y postest es de 2,48 y 1,98 respectivamente, en una escala de valoración de 1 a 5, disminuyendo su percepción de seguridad (ver **Tabla 140**).

- Percepción descargas ilegales

Otro de los contenidos dónde más se ha incidido ha sido en la percepción que tienen los jóvenes sobre la descargar de materiales con derechos de autor y copyright. En éste sentido, se han hallado mejoras significativas en la intervención (Z=-2,117; p=0,034), obteniendo una diferencia de medias entre el pretest y el postest de 3,05 y 2,54 respectivamente (Ver **Tabla 141**)

- Relación percepción burla – Personas que se han burlado

Se ha analizado la existencia de posibles relaciones entre las personas que en alguna ocasión se han burlado de la foto o comentario de otras personas, en redes sociales, y la percepción que tienen los jóvenes sobre la humillación en ellas. Como

hemos explicado anteriormente, la comprensión del acoso online, así como conocer la percepción del daño de las personas que humillan o insultan a otras personas a través de la red proporciona información de interés que nos permitiría desarrollar métodos de intervención eficaces para hacer frente al problema, el ciberbullying.

Los resultados nos muestran que en el pretest del grupo experimental existen evidencias de la relación existente entre ambas variables al resultar la prueba U de Mann-Whitney (U de M-W: 423,5; Z=-2,310; p=0,021). Se puede apreciar en el siguiente informe, donde las medias obtenidas en la escala de Likert sobre la percepción que tienen los jóvenes de la humillación online varían significativamente dependiendo de la respuesta obtenida a la pregunta ¿Alguna vez te has burlado de un comentario o foto en una red social?

No obstante, no ocurre lo mismo en el grupo control y en el postest de ambos grupos, por lo que no podemos concluir la existencia de una relación firme entre ambas variables. Sin embargo, sería recomendable analizarla nuevamente en estudios posteriores.

Resumiendo, tras el análisis de la eficacia de la intervención hemos hallado mejoras significativas en los resultados obtenidos en el postest respecto a los obtenidos en el pretest en:

- Configuración de las opciones de privacidad y seguridad de las redes sociales.
- Compartir fotos o vídeos con personas conocidas en internet.
- Percepción de seguridad en chats públicos

- Percepción descargas ilegales

Además, se observan mejoras no significativas, por lo que sería conveniente analizarlas en futuros estudios en el uso de software de protección y de la webcam con personas conocidas a través de la red.

3.4.2. Relaciones significativas entre variables halladas en el Postest

Relación entre configuración de la seguridad y modificación de la configuración de seguridad

Del mismo modo que en el análisis mostrado anteriormente, se pretende analizar la asociación entre la percepción de necesidad de configurar la seguridad y privacidad de las redes sociales y su modificación o revisión, tras la intervención.

Por tanto, a continuación, analizamos la relación existente entre las personas que han configurado la configuración de seguridad y privacidad de su red social y la percepción de la necesidad de ser ellos mismos quienes la configuren.

Podemos observar en la **Tabla 146** que el 65,2% de las personas que consideran necesario ser ellas mismas quienes configuren la seguridad y privacidad de sus redes sociales, afirman haber revisado la configuración de sus cuentas en el último mes. Sin embargo, aquellas personas que no lo consideran necesario no han revisado la configuración de sus redes sociales.

Además, la prueba de chi-cuadrado confirma que existe asociación entre estas dos variables (Chi-cuadrado: 14,047; gl: 1; $p<0,001$). Por tanto se puede afirmar, que

hay relación entre las personas que consideran necesario configurar ellas mismas la privacidad y seguridad de sus redes sociales y aquellas que han revisado o modificado la configuración tras la intervención (véase **Tabla 147**)

Relación entre antivirus y tener o no un antivirus en el móvil

La consideración que tienen los jóvenes sobre la importancia de tener instalado software de protección instalado en ordenadores, tabletas o smartphone puede estar asociada a la instalación de éste tipo de software en sus dispositivos de conexión a internet. Del mismo modo que hemos explicado con anterioridad, la comprensión de las decisiones tomadas por los jóvenes y de los riesgos a los que se exponen, nos aportan información relevante para la elaboración de intervenciones más eficientes. Por ello, hemos analizado la existencia de asociaciones entre la instalación de software de protección en los principales dispositivos de conexión a internet y la percepción del valor que tienen los jóvenes sobre su instalación.

En el siguiente informe, podemos observar que las respuestas de los que dijeron que sí tienen instalado software de protección en su smartphone se condensan en los valores altos de la escala de la pregunta 'Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador tablet y Smarphone', estándo concentrados entre los valores del 3 al 5 de la escala Lickert empleada. Mientras, aquellos que no tienen instalado software de protección en su Smartphone tienen respuestas más dispersas entre todos los valores disponibles, es decir, están repartidos del 1 al 5 (véase **Tabla 148**)

Finalmente, la prueba U de Mann-Whitney (véase **Tabla 149**) indica que existe relación entre las variables analizadas (U de M-W: 741,5; Z=-2,37; p=0,018).

3.4.3. Género como variable independiente en el postest

En éste apartado analizaremos si la variable género es significativa en la exposición a riesgos, en los resultados obtenidos en el postest.

En las pruebas realizadas en la variable género como variable independiente refleja que en la mayor parte de las asociaciones analizadas no existen diferencias significativas, excepto en los casos que se exponen a continuación:

Comentarios en redes sociales

La percepción de los jóvenes sobre la calidad de sus comentarios en redes sociales obtiene resultados desiguales entre los grupos. El grupo de control (Chi-cuadrado: 1,576; gl: 1; p=0,209) y el total de la muestra (Chi-cuadrado: 0,599; gl: 1; p=0,439) no hayan diferencias entre los chicos y las chicas. Sin embargo, no ocurre lo mismo con el grupo experimental que haya diferencias significativas entre ambos géneros (Chi-cuadrado: 5,291; gl: 1; p=0,021) debido a que la proporción de mujeres que dicen no tener comentarios inadecuados en sus redes sociales, 90,3%, es superior al de los hombres, 65,4%. Ver **Tabla 151**.

Percepción en la humillación en redes sociales

En el grupo de control, el análisis de las variables que usan escala Likert, nos muestran que existe relación significativa con el género, es decir, que los resultados son significativos entre hombres y mujeres respecto a la afirmación: Insultar, o vacilar, a

un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona. En la tabla de contingencia (véase **Tabla 154**) podemos ver que los hombres tienen puntuaciones más altas (media: 2,76, mediana: 3) que las mujeres (media: 1,79, mediana: 1). Es decir, la media de hombres están más de acuerdo con la afirmación planteada que las mujeres. Esta diferencia es estadísticamente significativa (U de M-W:152,500; Z=-2,422; p=0,015). Ver **Tabla 155**.

Páginas web adaptadas a la edad

El grupo experimental y el total de la muestra, se han encontrado diferencias significativas en la asociación de la variable género con el acceso a páginas web recomendadas para mi edad. En la **Tabla 156**, correspondiente al grupo experimental, se aprecia que los hombres obtienen una media de 2,72, con mediana 3, mientras que la media de las mujeres es de 3,69, con mediana 4. De igual modo, en la tabla **Tabla 158**, correspondiente al total de la muestra, observamos que la media de los hombres es de 2,72 y la de las mujeres es de 3,37, ambos con mediana 3.

Además, como indicábamos los resultados arrojados por la prueba U de Mann-Whitney reflejan que las diferencias son significativas en el grupo experimental (U de M-W:293,0; Z=-2,679; p=0,007) y el total de la muestra (U de M-W:1065,500; Z=-2,300; p=0,021). Por lo tanto, los hombres podemos afirmar que acceden más que las mujeres a páginas web con contenidos no adaptados a su edad lo que les expone a los riesgos derivados del acceso a contenidos inadecuados. Ver **Tabla 157** y **Tabla 159**.

Chats públicos

En el grupo de control, la percepción de seguridad en los chats públicos obtiene resultados diferenciados respecto a la variable género. En la **Tabla 154** se observa que la media de los hombres es de 1,62, con mediana 3, y la media de mujeres es 2,38, con mediana 2. Es decir, la percepción de la seguridad de los chats públicos de las mujeres es mayor que la de los hombres si observamos la media, sin embargo, la mediana nos muestra que la mitad de las mujeres están o en total desacuerdo o bastante desacuerdo con la afirmación planteada. Además, en la **Tabla 155** se aprecia que la relación entre hombres y mujeres respecto a la percepción de seguridad en los chats públicos está próxima a resultar significativa, lo que podría resultar significa en una muestras de mayor tamaño (U de M-W:173,5; Z=-1,904; p=0,057).

Se concluye por tanto que la variable género es significativa en el estudio de los hábitos en el uso de las TIC, dado que se obtienen asociaciones con otras variables, tanto en el pretest como en el postest. Además, tras la intervención se han encontrado diferencias significativas entre los hombres y las mujeres, en los hábitos mencionados, que no se hallaron anteriormente en el pretest.

CAPÍTULO V. DISCUSIÓN Y CONCLUSIONES

1. Discusión

En la última década han nacido múltiples iniciativas en beneficio de la seguridad de los jóvenes cuando utilizan las TIC: el programa Safer Internet, dónde destacamos el trabajo realizado en EU Kids Online, la estrategia europea para crear 'una mejor internet para los niños', eNACSO que trabajan para conseguir un entorno on line más seguro para los menores defendiendo sus derechos en la red, INHOPE a través de las líneas de denuncia, la oficina de seguridad del internauta, la creación de Inteco e Incibe, la adaptación de la legislación española, el incremento de los contenidos sobre seguridad en el uso de las TIC en el nuevo currículo LOMCE, etc.

Examinar las principales políticas y programas, nacionales y promovidos por la comisión europea, en beneficio de la seguridad de los jóvenes cuando hacen uso de las TIC, analizar los riesgos detectados que derivan de su uso y conocer el estado actual del problema, nos permite comprender la complejidad de la situación y la necesidad de intervenir con todos los medios a nuestro alcance para convertir internet y el uso de las TIC en una experiencia positiva y segura para nuestros jóvenes.

Todos los planes, proyectos e iniciativas que hemos podido examinar, se han convertido en los cimientos de la lucha contra los riesgos derivados del uso de las TIC y en defensa de los derechos de los jóvenes, que nos permiten comprender mejor el problema al que nos enfrentamos hoy en día. Sin embargo, como decimos, son los cimientos, es el comienzo de un largo camino pedregoso que nos hará enfrentarnos a

nosotros mismos y nuestros propios intereses en beneficio de la seguridad de nuestros niños y nuestros jóvenes.

A lo largo de la revisión literaria hemos podido examinar las principales medidas tomadas por los actores implicados, encaminadas a hacer frente a los riesgos que derivan de las tecnologías de la información y la comunicación. En la Figura 50, apreciamos de forma gráfica la situación de los niños y jóvenes, en el centro de políticas, discursos e iniciativas que les permitan disfrutar de los beneficios y oportunidades que tienen las TIC.

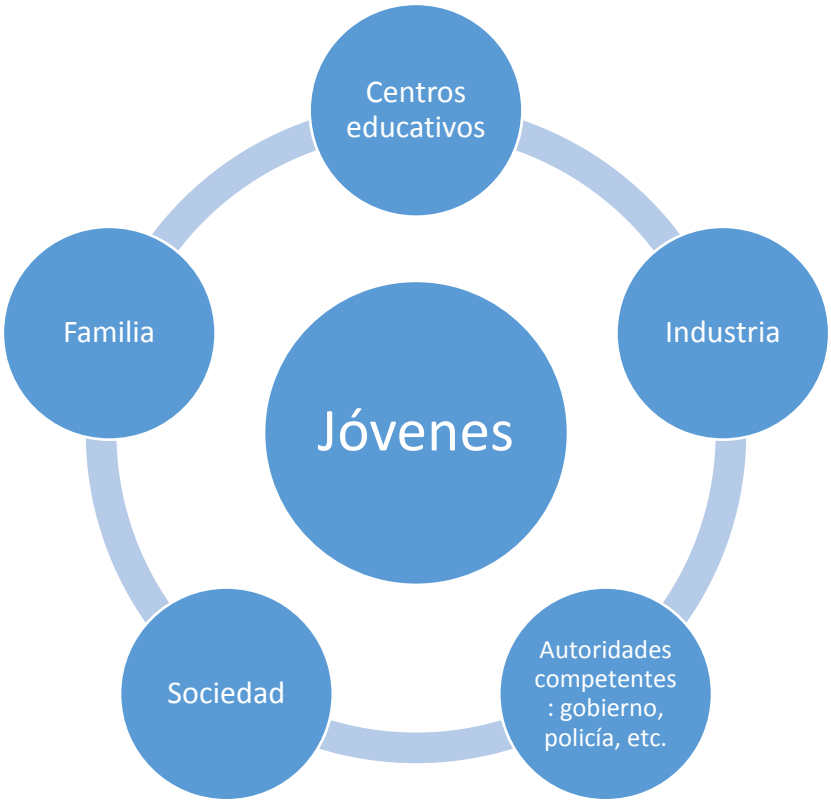


Figura 50 Situación de los jóvenes respecto a las TIC

Por último, todos los actores que posibilitan que los jóvenes hagan uso de las TIC deben responsabilizarse de la realidad que viven los menores al acceder a ellas e implicarse en hacer frente a las consecuencias nocivas que derivan de su uso. La

necesidad de adquisición de hábitos seguros y responsables se pone de manifiesto en los hábitos que actualmente tienen jóvenes y que les exponen a los riesgos derivados de las TIC. Del mismo modo que organizaciones públicas y privadas han acudido al auxilio de los jóvenes una vez se han detectado situaciones que pueden afectarles, las TIC han llegado a los hogares españoles apoyados por campañas de marketing dirigidas a la contratación y consumo, sin responsabilizarse de los riesgos derivados de su uso.

Además, hemos analizado los riesgos detectados que se han consolidado en el uso de las TIC, los hemos destripado para comprender su funcionamiento y existencia, y por su puesto para conocer las medidas que debemos tomar para evitar exponernos a ellos. Incluso hemos podido conocer, otros riesgos que han nacido con la evolución de las TIC, como es el caso de los juegos de realidad aumentada cuya supervivencia o evolución está por ver.

Sin embargo, como podremos apreciar, todo el esfuerzo realizado no ha logrado evitar que los jóvenes se expongan a los riesgos derivados de las TIC. Al inicio de la investigación los participantes muestran hábitos que les exponen a los riesgos analizados en el estudio que derivan del uso de las tecnologías de la información y la comunicación. Las destrezas y habilidades digitales que poseen los jóvenes, les permiten disfrutar de las oportunidades que ofrecen las TIC y hacer uso de aplicaciones y recursos web, sin embargo, sus hábitos seguros y responsables no han evolucionado al mismo ritmo.

Es significativo que el 42,1% de los participantes afirman que no han hablado con nadie sobre los hábitos saludables que les protejan de los riesgos derivados del uso de las TIC. Ver **Tabla 6** En este sentido, el alumnado carece de oportunidades que les

permitan desarrollar hábitos seguros y responsables, al mismo tiempo que desarrollan sus habilidades digitales, lo que les posiciona en situación de vulnerabilidad.

Los centros escolares, emplazados en una situación privilegiada, para fomentar y sensibilizar a los jóvenes en la adquisición de hábitos seguros y responsables en el uso de las TIC, se han enfrentado en la última década a una transformación integral debido a la irrupción de las TIC en el aula. Conscientes de la necesidad formativa de los jóvenes en éste sentido, han ido integrando las TIC progresivamente en el centro, fomentando el desarrollo de las competencias digitales del alumnado. Sin embargo, los jóvenes que aprenden a utilizar las tecnologías con gran habilidad, están adquiriendo determinados hábitos que les exponen a los riesgos derivados del uso de las TIC. Es por ello, que los centros educativos deben implicarse para que los jóvenes sean capaces de desarrollar sus hábitos seguros y responsables al mismo tiempo que adquieren competencias digitales que les permiten hacer uso de las oportunidades que proporcionan las TIC.

En la vida cotidiana utilizamos etapas de aprendizaje, que son especialmente visibles en los más pequeños, cuando comienzan a desarrollar destrezas que les permiten adquirir mayor autonomía. Es conocido por todos que los más pequeños necesitan que las personas adultas les muestren la forma correcta de realizar determinadas actividades o utilizar utensilios sin ponerse en riesgo. Nadie se escandalizaría si vemos a un niño que aprende a montar en bicicleta con ayuda de sus padres, quienes establecen etapas de aprendizaje hasta que el joven es capaz de montar sin la supervisión paterna o materna. Del mismo modo, si queremos que un niño aprenda a utilizar un cuchillo para comer, inicialmente le explicaremos como utilizarlo adecuadamente, mostrándole el modo seguro de uso y advirtiéndole de los riesgos

derivados del uso incorrecto. Tampoco le daríamos un cuchillo muy afilado o que se pueda pinchar, sino que le daríamos el cuchillo menos peligroso que tengamos en la cocina y, aun así le supervisaríamos para asegurarnos que lo utiliza de forma adecuada. Estas etapas de aprendizaje, que terminan en el momento en que el joven hace un uso seguro y responsable del mismo, deben utilizarse con el aprendizaje y uso de las TIC que presenten riesgos que puedan afectar a los jóvenes. Sin embargo, los jóvenes que adquieren destrezas digitales en el centro educativo, aprenden por ellos mismos a utilizar las TIC que ofrecen oportunidades de comunicación, diversión, etc. Adquieren hábitos, transferidos a través de sus iguales, que consideran adecuados para su uso y disfrute, sin gozar del acompañamiento recomendado para evitar la adquisición de conductas que les expongan a los riesgos que derivan de ellos. Es por ello, que los jóvenes muestran carencias en el uso seguro y responsable de las TIC, que les sitúa en una posición vulnerable y que les expone a los efectos nocivos que derivan de su uso.

En éste sentido, el esfuerzo realizado con la incorporación de las TIC en el currículo y por los centros educativos no es suficiente. La escasez de contenidos sobre seguridad en el uso de las TIC en los currículos escolares que permitan a los jóvenes adquirir hábitos saludables al mismo ritmo que desarrollan sus destrezas digitales, les posiciona en situación de vulnerabilidad al quedar expuestos a los riesgos derivados del uso de las TIC. Se debe señalar que, en éste sentido, la significación que ha adquirido la seguridad en uso de las TIC en la reciente ley para la mejora de la calidad educativa, la LOMCE, puede implicar mejoras en los hábitos seguros y responsables de los jóvenes. No obstante, debido a los constantes cambios que ofrece el comercio tecnológico, los jóvenes deben aprender a analizar desde un punto de vista de la seguridad las aplicaciones y dispositivos que utilizan. No hay que olvidar que los riesgos derivados

del uso de las TIC son cambiantes, es decir, los que conocemos a día de hoy pueden desaparecer, cambiar o aparecer otros nuevos riesgos según evolucionen las TIC y las oportunidades que nos ofrecen. Sin ir más lejos, un ejemplo reciente, fue la llegada de Pokemon Go. Supuso la oportunidad, para muchos jóvenes, de utilizar por primera vez la realidad aumentada. Sin embargo, del mismo modo que permite a los usuarios disfrutar de la conexión entre el mundo virtual y el mundo físico a través del dispositivo móvil, las autoridades policiales han visto la necesidad de realizar campañas advirtiendo de los riesgos de uso (El Mundo, 2016).

2. Conclusiones

1. La implementación de un plan adecuado de intervención para desarrollar hábitos seguros y responsables en el uso de las TIC disminuye la exposición a los riesgos derivados del uso de las TIC.

   El efecto del plan de intervención diseñado para desarrollar los hábitos seguros y responsables en el uso de las TIC, analizado según la modalidad de intervención (experimental vs. control), fue positivo porque supuso el favorecimiento de los hábitos seguros y responsables de los jóvenes, disminuyendo la exposición a riesgos derivados del uso de las TIC.

   La mejora experimentada en los hábitos seguros y responsables que han sido favorecidos, difiere según los tipos de hábitos que analicemos. Es decir, la intervención ha obtenido resultados que muestran la disminución de la exposición en algunos de los riesgos que forman parte del estudio, mostrándose ineficaz para el resto de riesgos analizados. Concretamente, tras el análisis de la eficacia de la intervención se han hallado mejoras significativas en las variables que se exponen a continuación.

   1.1 La intervención aumenta el interés de los jóvenes de configurar las opciones de privacidad y seguridad de sus redes sociales. Según podemos ver en la **Tabla 118**, de la página 379, tras la intervención aumentan considerablemente los jóvenes que consideran necesario revisar o modificar las opciones de privacidad y seguridad de sus redes sociales.

   1.2 El tratamiento realizado consigue que disminuyan los jóvenes que muestran predisposición en compartir fotos o vídeos con personas conocidas en

internet. En la **Tabla 124**, de la página 384, se observa que la predisposición de los jóvenes a compartir fotos o vídeos con personas conocidas en internet, disminuye significativamente tras la intervención. Antes de la intervención se observa que los jóvenes muestran mayor predisposición a compartir fotos o vídeos personales, con personas que han conocido en internet, que tras la intervención.

1.3 Aumenta la percepción de los riesgos derivados del contacto con desconocidos a través de los chats públicos. En la **Tabla 141**, de la página 399 , podemos ver que, las sesiones recibidas les permiten percibir los riesgos derivados del contacto con personas desconocidas en los chats públicos, obteniéndose la disminución de la percepción de seguridad en ellos con respecto a los resultados hallados en antes de la intervención.

1.4 La formación en hábitos seguros y responsables en el uso de las TIC permite mejorar la percepción que tienen los jóvenes sobre las descargas ilegales. Según podemos ver en la **Tabla 141**, de la página 399 los jóvenes aumentan su comprensión sobre las consecuencias de la descarga de materiales con derechos de autor, con respecto a los resultados obtenidos antes de la intervención.

1.5 Los jóvenes que reciben el tratamiento revisan o modifican la configuración de seguridad y privacidad de sus redes sociales. En la **Tabla 144**, de la página 402, se observa que los jóvenes revisan la configuración de seguridad y privacidad de sus redes sociales tras las sesiones recibidas.

2. Los jóvenes participantes en la investigación muestran carencias en los hábitos seguros y responsables en el uso de las TIC, anteriormente a la implementación del programa de intervención.

   Previamente a la aplicación del plan de intervención, los participantes muestran hábitos que les exponen a los riesgos que derivan de uso de las TIC, si bien, la exposición se produce de manera desigual según los riesgos a los que nos refiramos. Por tanto, los hábitos que han adquirido los jóvenes en el desarrollo de las competencias digitales muestran carencias en la seguridad con la que hacen uso de las TIC.

   2.1 Las necesidades detectadas en los hábitos seguros y responsables adquiridos se pueden explicar, entre otros motivos, por la escasez de contenidos sobre seguridad en el uso de las TIC en los currículos escolares, en los que se prima la adquisición de habilidades y destrezas en el uso de las TIC. Por ello, se debe apostar por un currículo en el que se fortalezca y se desarrollen los hábitos seguros y responsables a la vez que los jóvenes adquieren habilidades y destrezas digitales que les permitan utilizar las TIC de forma autónoma.

   2.2 Las carencias detectadas ponen de manifiesto conductas poco responsables que les exponen a riesgos, bien por baja valoración de las consecuencias o por desconocimiento de las mismas. No obstante, debido a la importancia que adquiere la toma de decisiones en la exposición a los riesgos derivados del uso de las TIC, los jóvenes se deben responsabilizar de sus decisiones y tomar conciencia de su importancia. Todo ello, lo podemos apreciar en las variables analizadas, por ejemplo: en la **Tabla 8**, donde se muestran los

contactos que los jóvenes aceptarían en sus redes sociales; la **Tabla 22**, en la que podemos ver las personas dispuestas a compartir fotos o vídeos personales con conocidos en internet; o en la **Tabla 16**, donde se ve los jóvenes que no consideran necesario revisar o modificar su configuración de redes sociales.

2.3 Los jóvenes muestran gran predisposición en la exposición de información personal. La exposición de información personal es uno de los principales desencadenantes de exposición a los riesgos que derivan de las TIC y, sin embargo, en los hábitos que muestran los jóvenes no se observa que se tomen las medidas adecuadas que les proteja de los efectos nocivos que conllevan. Se ha recogido información al respecto, en diversas variables, siendo visible, por ejemplo, en la **Tabla 10**, donde se aprecia el volumen de fotos personales que tienen compartidas en las redes sociales, o en la **Tabla 22**, donde se aprecia una proporción significativa de jóvenes que están predispuestos a compartir fotos personales con personas conocidas en internet.

3. Los jóvenes que han recibido información sobre hábitos seguros y responsables, anteriormente a formar parte de la investigación, se exponen en menor medida a algunos de los riesgos analizados que aquellos que nunca recibieron información de este tipo.

   - Los jóvenes que recibieron información sobre hábitos seguros y responsables en el uso de las TIC, previamente a la intervención, permiten el acceso a sus redes sociales a personas más cercanas y conocidas que los que nunca han recibido información de este tipo. En la **Tabla 78**, de la página 346, se aprecia que los

jóvenes que han recibido información sobre hábitos seguros y responsables en el uso de las TIC tienden a ser más selectivos con los contactos que agregan a sus redes sociales, añadiendo a personas más cercanas, que los jóvenes que no han recibido este tipo de información.

- Los jóvenes que han recibido información sobre hábitos seguros y responsables, se burlan menos de otras personas que los que no han recibido información. En la **Tabla 104**, de la página 360, podemos ver que los jóvenes que han recibido este tipo de información, mayoritariamente, niegan haberse burlado de alguna foto o comentario en redes sociales, a diferencia de aquellos que nunca han recibido información sobre hábitos seguros y responsables en el uso de las TIC. Sin embargo, la información recibida no ha mostrado ser igual de eficiente en el resto de los hábitos analizados.

4. La variable género ha resultado ser significativa en la exposición a riesgos derivados del uso de las TIC. Sin embargo, la significación del género en nuestro estudio se muestra de manera desigual entre la exposición a unos u otros riesgos.

   Tras la intervención con el grupo experimental, se encontraron diferencias significativas en la exposición a riesgos que experimentan los jóvenes en función del género de los mismos. Los casos más relevantes que se han hallado son los siguientes:

   - En la **Tabla 150**, de la página 406, observamos que los jóvenes afirman tener más comentarios inadecuados que las mujeres.
   - La **Tabla 156**, de la página 412, se muestra que los hombres acceden a páginas no adaptadas a su edad, en mayor proporción que las mujeres.

- En la **Tabla 154**, de la página 410, se ve que los hombres tienen mayor percepción de seguridad en los chats públicos que las mujeres, quienes perciben mejor los riesgos que presentan el contacto con desconocidos a través de este medio.

5. Las acciones encaminadas al desarrollo de los hábitos seguros y responsables en el uso de las TIC, promovidas por los actores implicados, no han logrado evitar, que los jóvenes de 2º de la ESO de los centros educativos participantes en el estudio, se expongan a los riesgos derivados de su uso.

   Los resultados obtenidos previamente a la aplicación del plan de intervención, destacando los comentados anteriormente en la conclusión 2, nos muestran los hábitos seguros y responsables de los jóvenes en el uso de las TIC. En ellos podemos observar que la exposición a los riesgos que derivan del uso de las TIC, les sitúa lejos de los hábitos seguros y responsables que les permitan aprovechar las oportunidades que ofrecen las TIC sin exponerse a los riesgos derivados de su uso.

3. Limitaciones del estudio

Las limitaciones de este estudio deben buscarse en la naturaleza del propio estudio, el tamaño de la muestra seleccionada, el tipo de muestreo, el contexto en el que se ha realizado la investigación, los posibles sesgos del alumnado y del investigador, así como las limitaciones propias del método de investigación empleado.

El estudio puso en marcha un cuasi-experimento que se desarrolló en un contexto natural como es un centro educativo. Las propias condiciones para realizar un experimento en una situación real repercutieron en la aleatorización de la muestra, que se tuvo que hacer con cierta flexibilidad.

El tamaño de la muestra, compuesta por un total de 107 jóvenes puede considerarse adecuada para dotar de validez científica al estudio. Sin embargo, debido al tamaño de la muestra no es posible extrapolar los resultados obtenidos al resto de la comunidad escolar. Del mismo modo, el tipo de muestreo utilizado, disponible y no representativo, tampoco hace aconsejables las generalizaciones, puesto que los datos obtenidos sólo tienen significado para el propio centro. Únicamente, podría valorarse la generalización con jóvenes y centros con las mismas características. Aun así, los hallazgos encontrados tienen interés educativo y pueden servir de punto de partida para la realización de futuros estudios en contextos educativos.

Las preguntas incluidas en los cuestionarios nos permiten recoger información sobre los hábitos de los jóvenes que les exponen a los riesgos incluidos en el estudio que derivan del uso de las TIC. Es posible que jóvenes que no tienen determinado hábitos nocivos, se expongan a los riesgos a través de otros hábitos. No obstante, las

variables empleadas nos permiten conocer los hábitos de los jóvenes que se han considerado más relevantes en el estudio y el efecto de la intervención sobre ellos.

Respecto a los posibles sesgos del alumnado, éstos pudieron producirse al realizar el alumnado individualmente el cuestionario de hábitos seguros y responsables en el uso de las TIC, antes y después de la intervención, con lo que los resultados han podido estar condicionados por las respuestas socialmente aceptables. En relación con el investigador, al coincidir con el aplicador del plan de intervención, no se descarta la posibilidad de que los resultados no estén exentos de sesgos. No obstante, se decidió que el investigador y el administrador del programa fueran la misma persona para evitar posibles condicionamientos de los resultados finales.

Por su parte, la metodología cuantitativa que se ha utilizado tiene sus propias limitaciones al centrarse en la cuantificación de los hechos sin tener en cuenta los significados internos de los fenómenos, por lo que puede dificultarse la comprensión de los mismos. De este modo, la metodología cuantitativa busca medir los hechos más que intentar explicar porqué se producen, con lo que la información obtenida a través de este enfoque adolece de validez ecológica.

4. Aportaciones y líneas futuras de investigación

Las aportaciones de esta investigación revierten en el desarrollo de los hábitos seguros de los jóvenes cuando utilizan las TIC, convirtiendo a los jóvenes en los principales actores en la relación máquina-persona al ser ellos mismos quienes toman las decisiones de manera autónoma.

Las TIC, por su propia naturaleza, no cesan de evolucionar, surgiendo nuevos dispositivos y aplicaciones, que según sus características y del uso que se haga de ellas pueden resultar beneficiosas o dañinas para los jóvenes. Los centros educativos están situados en una posición privilegiada que les permite dotar a los jóvenes de los conocimientos y herramientas necesarias para que sean capaces de hacer frente a los riesgos que derivan del uso de las TIC. En éste sentido el propio centro debe generar mecanismos e iniciativas que favorezcan las adquisición de hábitos seguros y responsables en el uso de las TIC e implicar a todos los profesionales del centro educativo que deben transmitir un mismo mensaje dirigido a este fin. Es necesario tener en cuenta que la llegada del nuevo currículo LOMCE incrementa el valor aportado a la formación y sensibilización en seguridad en el uso de las TIC, lo que dibuja un nuevo escaparate en los próximos años que sin duda se diferenciará del visto en la presente investigación.

Incorporar en el plan de intervención acciones dirigidas a la mediación parental en el ámbito de la seguridad en el uso de las TIC podría conseguir efectos positivos que mejoren los resultados obtenidos hasta el momento. Los padres, madres y demás familiares que se ocupan de la educación de los menores en ocasiones se ven

desbordados por la rapidez con la que evolucionan las TIC y no son capaces de adquirir las habilidades necesarias para utilizarlas y conocer los riesgos derivados de su uso. Es necesario recordar que aún nos encontramos en un momento de transición, en el que los jóvenes nativos digitales aprenden con mayor facilidad a utilizar las TIC que sus padres y madres. Esto puede derivar en que los jóvenes no vean a sus familiares como personas de referencia a las que puedan acudir para preguntarles dudas sobre el uso adecuado de las TIC o compartirles experiencias que no sepan abordar. Las familias, los padres y las madres, han de encontrar el medio para formar parte de la vida digital de sus hijos, educándoles sobre un uso seguro de las TIC y convertirse en las personas de referencia para ellos, también en el ámbito digital.

Además, como hemos visto anteriormente, no son los únicos actores que deben implicarse en ésta ardua tarea, sino que la industria debe generar herramientas, aplicaciones y dispositivos seguros para los jóvenes, que faciliten la denuncia de conductas inapropiadas, o de riesgos para otros usuarios, u otro tipo de actuaciones que protejan a los menores.

El estudio de la evolución de los hábitos seguros y responsables en el uso de las TIC se antoja imprescindible en los próximos años. Sin duda, la llegada de la LOMCE puede resultar significativa, sin embargo, debido a la complejidad del problema se observa necesaria la participación de otros actores externos al centro educativo que implementen y evalúen planes de intervención con los jóvenes, con las familias y con el profesorado, con el fin de beneficiar la seguridad de los jóvenes cuando hacen uso de las TIC.

La inclusión de nuevas variables podría plantear nuevas hipótesis que nos permitan entender mejor el problema, la realidad de cada aula y de éste modo plantear nuevos planes de intervención que mejoren los resultados obtenidos. Hasta ahora, se ha visto en otros estudios realizados que la edad, el sexo e incluso el estatus socioeconómico son variables significativas en la exposición a riesgos. Otra variable a tener en cuenta, especialmente en los países y regiones con altas tasas de inmigración, es la significación del país de procedencia. El alumnado de centros educativos con altas tasas de población procedente de otros países pueden experimentar exposiciones a riesgos que difieran de los resultados obtenidos en centros con diferentes características.

La investigación pone de manifiesto la necesidad de sensibilizar a los jóvenes sobre las consecuencias nocivas del uso de las TIC. Enseñarles a utilizarlas de forma positiva sin exponerse a riesgos debe convertirse en una prioridad de los centros educativos, aunque la realidad es que en ocasiones los propios centros no saben cómo afrontar el problema, o bien, no le dan el valor suficiente para crear un plan de intervención integral que incluya a los profesionales del centro educativo, a las familias y, por supuesto, al alumnado.

Si bien, la presente investigación se centró en los jóvenes de 2º de la ESO, sería muy conveniente incluir a menores desde edades tempranas hasta cumplir la mayoría de edad. Hay investigaciones que afirman que la edad del comienzo del uso de las TIC es de 7 años. En éste caso, habría que conocer previamente los riesgos a los que se exponen los más pequeños, que dependerá del uso que hagan de las TIC y de sus habilidades digitales. También la intervención, metodología y dinámicas que se trabajen en el aula, con este fin, han de estar dirigidas y adaptadas a la edad de los participantes,

teniendo en cuenta los riesgos a los que se exponen, ya que en caso contrario podrían obtenerse efectos adversos como transmitir temor o rechazo a las TIC.

Otro aspecto a tener en cuenta es la metodología expositiva y participativa utilizada en el aula en las sesiones realizadas en los centros educativos en nuestra investigación. Es necesario plantearse nuevas metodologías y otros planteamientos que propicien la obtención de nuevos y mejores resultados.

Tras la intervención en uno de los centros educativos que han formado parte de la investigación, la dirección del centro con nuestro apoyo y asesoramiento, se formó un grupo de expertos en seguridad TIC, formado por alumnos/as del centro que durante el año en curso se encargarían de ofrecer apoyo e información al resto de alumnado del centro que pudiese precisar asesoramiento o apoyo en el uso de las TIC. Además, realizaron labores de formación en hábitos seguros y responsables en el uso de las TIC en algunas de las líneas que se valoró necesario. Durante el tiempo en el que intervino el grupo de expertos, les dimos apoyo y asesoramiento, aunque se desconocen los efectos de la intervención. No obstante, la experiencia ha sido positiva tanto para el alumnado que ha intervenido, como para el centro educativo cuyo alumnado recibió información sobre las TIC a manos de éstos incipientes expertos. Aunque se ha tratado de un proyecto piloto, en el que se desconocen los efectos, abre una nueva vía de actuación.

Los estudios sobre los hábitos de los jóvenes al usar las TIC se inscriben en un campo de estudio en boga y con una gran proyección por las implicaciones económicas, políticas, sociales, culturales y educativas que tienen en las sociedades contemporáneas. A pesar de ello, se observa escasez de estudios sobre intervenciones realizadas en centros educativos y con familias, por lo que la presente tesis puede guiar futuras

investigaciones que se emprendan sobre ésta temática. En éste sentido, las conclusiones obtenidas pueden ser el punto de partida de otras investigaciones que se lleven a cabo en ámbitos educativos y que desde prismas distintos aporten elementos para apoyar o refutar las hipótesis y planteamientos de este estudio.

5. Síntesis

La interpretación de los resultados y el establecimiento de conclusiones supone el punto culminante de cualquier investigación. En un estudio en donde prima la metodología cuantitativa y, por tanto, la presencia de datos numéricos es abundante, debe dotarse de sentido a todo el volumen de información recopilada, si se pretende explicar y comprender el fenómeno educativo estudiado desde un planteamiento riguroso y científico. Los resultados de la presente tesis aportan datos de interés práctico. Revelan el impacto positivo que ha tenido la implementación de un plan para el desarrollo de los hábitos seguros y responsables en el uso de las TIC en el alumnado de 2º de la ESO. Además, los hallazgos indican diferencias significativas en la exposición a riesgos derivados del uso de las TIC según el género de los jóvenes, así como los hábitos seguros que muestran los jóvenes que han recibido información sobre seguridad en el uso de las TIC, previamente a la intervención, a diferencia de aquellos que no la han recibido.

Las conclusiones obtenidas permiten establecer futuras líneas de trabajo que profundicen en el conocimiento de los riesgos derivados del uso de las TIC y de los hábitos seguros que eviten la exposición a dichos riesgos de los menores, un campo de estudio de gran interés y proyección por las numerosas implicaciones que tiene en las sociedades actuales. Además, se debe tener en cuenta a todos los actores implicados, destacando el papel de los centros educativos quienes se sitúan en una situación privilegiada para dotar a los jóvenes de los conocimientos necesarios para evitar la exposición a los riesgos derivados del uso de las TIC. En este contexto, la integración de las TIC en los centros educativos del siglo XXI, en constante evolución debido a las

ventajas y oportunidades que presentan en la educación, dotarán a los jóvenes de las habilidades digitales necesarias para hacer frente a los retos formativos del presente y del futuro, en una sociedad donde las TIC están presentes en todos los ámbitos de nuestra vida.

CAPÍTULO VI: REFERENCIAS

Agència de Qualitat d'Internet en colaboración con la Associació contra l'Anorèxia i la Bulimia. (2010). *Las páginas "pro-ana" y "pro-mia" inundan la red.* Barcelona. Obtenido de http://www.f-ima.org/fitxer/403/resumen_informe_anorexia_y_bulimia_en_internet.pdf

Apple Inc. (2014). *Internet a Better Place For Children.* Informe de aplicación. Obtenido de http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=4416

Asociación Contra la Anorexia y la Bulimia de Cataluña. (02 de 2015). *Asociación Contra la Anorexia y la Bulimia de Cataluña*. Obtenido de http://www.acab.org/es/que-son-los-trastornos-de-la-conducta-alimentaria/recursos-sanitarios/asociaciones-espana/cataluna

Asociación Protégeles. (2014). *Protegeles*. Obtenido de http://www.protegeles.com/

BBFC. (1998). *British Board Film Clasification - Age Ratings you trust* -. Recuperado el 24 de 10 de 2015, de http://www.bbfc.co.uk/

Bottero, M., Escoto, L., y Goncálvez, S. (2006). Educación Social y Cívica. *Colección Estudiantil*.

Chamorro, R. (2001). El Plan de Acción INFO XXI. *Autores científico-técnicos y académicos*, 61-64.

Cloquell Lozano, A. (4 de 2015). Usos sociales de internet entre los adolescentes españoles. *Revista sobre la infancia y la adolescencia*(8), 1-14. doi:ISSN 2174-7210

Comisión Europea. (2010). *EUR-Lex - Access to European Union law -*. Recuperado el 14 de 10 de 2014, de http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:si0016

Comisión Europea. (1 de 12 de 2011). *Digital Agenda: Coalition of top tech & media companies to make internet better place for our kids.* Comunicado, Brussels.

Comisión Europea. (2012a). *European Commission.* Recuperado el 15 de 07 de 2014, de http://europa.eu/rapid/press-release_IP-12-445_es.htm

Comisión Europea. (2012b). *European Commision.* Recuperado el 21 de 07 de 2014, de Press Release Database: http://europa.eu/rapid/press-release_IP-12-1389_es.htm

Comisión Europea. (2013a). *Digital Agenda for Europe*. Recuperado el 16 de 09 de 2013, de A Europe 2020 Initiative: https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-36-support-reporting-illegal-content-online-and-awareness-campaigns

Comisión Europea. (2013b). *Digital Agenda For Europe.* Bruselas. Obtenido de A Europe 2020 Iniciative: https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-35-guidance-implementation-telecoms-rules-privacy

Comisión Europea. (02 de 09 de 2014). *Agenda Digital Para Europa*. Obtenido de http://ec.europa.eu/digital-agenda/en/news/ceo-coalition-2014-progress-reports-actions-make-internet-better-place-kids

Comisión Europea. (2014). *Balance de la Estrategia Europa 2020 para un crecimiento inteligente, sostenible e integrador*. Bruselas. Obtenido de http://ec.europa.eu/europe2020/pdf/europe2020stocktaking_es.pdf

Comisión Europea. (07 de 01 de 2015a). *Digital Agenda for Europe*. Obtenido de A Europe 2020 iniciative: http://ec.europa.eu/digital-agenda/en/digital-agenda-europe-2020-strategy

Comisión Europea. (07 de 01 de 2015b). *Digital Agenda For Europe*. Recuperado el 15 de 04 de 2015, de A Europe 2020 Iniciative: https://ec.europa.eu/digital-agenda/en/our-goals

Comisión Europea. (2015c). *Digital Agenda For Europe*. Recuperado el 2015, de A Europe 2020 Iniciative: https://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security#Our Actions

Comisión Interministerial de la Sociedad de la Información y de las Nuevas Tecnologías. (2000). *INFO XXI. La Sociedad de la Inform@ción para todos.* Obtenido de http://www.internautas.org/documentos/infoxxi.pdf

Comité de las Regiones. (2013). *Evaluación de la iniciativa emblemática: Una Agenda Digital para Europa.* Bruselas. Obtenido de https://portal.cor.europa.eu/europe2020/MonitoringFlagships/Documents/Digital%20agenda/cdr2107-2013_00_00_tra_tcd_es.doc

Comité de las Regiones. (2013). *Summary of a Survey on the Europe 2020.* Obtenido de https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCcQFjAAahUKEwiR0Pr5_eTGAhWRB9sKHQLhDqg&url=http%3A%2F%2Fcor.europa.eu%2Fen%2Fdocumentation%2Fstudies%2FDocuments%2Fsummary-survey-digital-agenda%2Fsummary-survey-eu2020-di

Committee of the Regions. (2013). *The EU's Assambly of Regional and Local Representatives*. Recuperado el 15 de 09 de 2013, de http://cor.europa.eu/en/news/events/Pages/europe-2020-conference-digital-agenda.aspx

Donoso, V. (2011). *Assesment of the implementation of the Safer Social Networking Principles for the EU on 14 websites.* Summary Report, European Commision, Safer Internet Programme, Luxembourg.

Egido, I., Aranda, R., R., C., de la Herrán, A., de Miguel, S., Gómez, M., y otros. (2006). Aprendizaje basado en problemas. Estrategia metodológica y organizativa del curriculum para la calidad de la enseñanza en los estudios de Magisterio. Revista Interuniversitaria de Formación del Profesorado, 20, 137-149.

El País. (21 de 03 de 2015). *Brasil preocupado por reclutamiento de jóvenes por parte del EI*. Obtenido de El Pais (Mundo): http://www.elpais.com.uy/mundo/brasil-preocupado-reclutamiento-jovenes-yihadistas.html

European NGO Alliance for Child Safety Online. (2014). *eNACSO.* Obtenido de www.enacso.eu/about-us/focus-areas

Estirado, L. (02 de 02 de 2015). Una madre clama por la prohibición de webs que fomentan la anorexia y la bulimia. *elperiodico*, págs. http://www.elperiodico.com/es/noticias/sociedad/madre-pide-changeorg-prohibir-webs-anorexia-bulimia-3902115. Obtenido de http://www.elperiodico.com/es/noticias/sociedad/madre-pide-changeorg-prohibir-webs-anorexia-bulimia-3902115

EU Kids online. (2014). *Eu Kids online: Findings, methods and recomdendations.* Recuperado el 07 de 07 de 2015, de http://lsedesignunit.com/EUKids Online/index.html?r=64

European Commission. (02 de 05 de 2012). *European Strategy for a Better Internet for Children.* COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Brussels. Obtenido de http://europa.eu/rapid/press-release_IP-12-445_es.htm

European Commission. (2013). *Digital Agenda For Europe*. Obtenido de Los Estados miembros deben crear líneas de contacto para denunciar la existencia de contenidos dañinos en la red.: http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-40-member-states-implement-harmful-content-alert-hotlines

European Commission. (04 de Junio de 2013). *Europe's top tech executives and Commission affirm commitment to collaborate, not compete to improve the internet for kids.* Bruselas. Recuperado el 15 de 01 de 2014, de http://europa.eu/rapid/press-release_MEMO-13-504_en.htm

European Commission. (2014). *Agenda Digital para Europa*. Obtenido de Action 125: Expand the Global Alliance against Child Sexual Abuse Online: https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-125-expand-global-alliance-against-child-sexual-abuse-online

European Commission. (23 de 10 de 2014). *Digital Agenda For Europe.* Obtenido de Project factsheets: Digital security: http://ec.europa.eu/digital-agenda/en/node/76649

European Commission. (18 de 03 de 2015a). *Digital Agenda For Europe.* Obtenido de Online Privacy: http://ec.europa.eu/digital-agenda/en/online-privacy

European Commission. (02 de 03 de 2015b). *Digital Agenda For Europe.* Obtenido de Cybersecurity: http://ec.europa.eu/digital-agenda/en/cybersecurity

European Commission. (23 de 06 de 2015c). *Digital Agenda for Europe*. Obtenido de A European Strategy to deliver a Better Internet for our Children: https://ec.europa.eu/digital-agenda/node/286

European Schoolnet. (2015). *Safer Internet Day 2015.* Luxemburgo. Obtenido de http://www.saferinternetday.org/c/document_library/get_file?uuid=fbf1c3a3-2192-45c9-a787-28d1b06bfc5e&groupId=10136

Ferguson, C. (2011). Sexting behaviors among Young Hispanic women: incidence and associating with other high-risk sexual behaviors. *PsychiatriQ*, 82 (3): 239-43.

Fundación Alia2. (2012). *Por un internet más seguro para nuestros hijos*. Recuperado el 24 de 05 de 2013, de http://alia2.org/

Fundación Alia2. (s.f.). *Alia2*. Recuperado el 24 de 10 de 2014, de http://alia2.org/

Fundación imagen y autoestima. (2013). *La apologia en internet: las páginas pro-ana y pro-mia.* Recuperado el 07 de 07 de 2015, de http://www.f-ima.org/es/trastornos-relacionados/factores-de-riesgo/la-apologia-en-internet-las-paginas-pro-ana-y-pro-mia

Fundacion imagen y autoestima. (2013). Protocolo denuncia proANA. Recuperado el 07 de 07 de 2015, de http://www.f-ima.org/es/trastornos-relacionados/factores-de-riesgo/la-apologia-en-internet-las-paginas-pro-ana-y-pro-mia

Fundación Imagen y Autoestima. (2016). *Fundación Imagen y Autoestima*. Obtenido de http://www.f-ima.org/es/

Garmendia, M., Garitaonandia, C., Martínez, G., y Casado, M. (2011). *Riesgos y seguridad en internet: Los menores españoles.* País Vasco. Obtenido de http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/National%20reports/Spanish%20report.pdf

Gentile, D., Maier, J., Hasson, M., & López de Bonetti, B. (2011). Parents evaluation of media ratings a decade afeter the television ratings were introduced. *Pediatrics*(128), 36-44.

Gómez, A. (Septiembre de 2011). Beyond good and evil the Spam. *Revista Modmex* PC, 12-14. Obtenido de http://revistamodmex.wordpress.com

García Gómez, M., Ferrer, R. y De La Herrán, A. (2015a). Las redes sociales verticales en los sistemas formales de formación inicial de docentes. Revista Complutense de Educación, 215-232.

Gómez García, M., Ruiz, J. y Sánchez, J. (2015b). Aprendizaje social en red. Las redes digitales en la formación universitaria. 4 (2), 71-87.

Grupo de Investigación EU Kids Online. (s.f.). *Universidad del País Vasco*. Recuperado el 15 de 03 de 2013, de http://www.ehu.eus/es/web/eukidsonline/eu-kids-online-ii

Grupo de Investigación EU Kids Online. (s.f.). *Universidad del País Vasco*. Recuperado el 17 de 03 de 2013, de http://www.ehu.eus/es/web/eukidsonline/eu-kids-online-iii

Haddon, L., Livingstone, S., & network, a. t. (2015). *EU Kids Online: Findings, methods and recommendations.* Recuperado el 02 de 08 de 2015, de http://lsedesignunit.com/EUKidsOnline/index.html?r=64

Haddon, Leslie, Livingstone, Sonia and the EU Kids Online network. (2012). *EU Kids Online: national perspectives.* EU Kids Online, The London School of Economics and Political Science, London, UK. Recuperado el 28 de 06 de 2014, de http://eprints.lse.ac.uk/46878/

Hasebrink, U., Olafsson, K., & Stetka, V. (2009). *Opportunities and pitfalls of crossnational research.* In S. Livingstone and L. Haddon, Kids Online: Opportunies and Risks for Children. Bristol: ThePolicyPress.

Hinduja, S., & Patchin, J. (2009). *Bullying beyond the schollyardd: preventing and responding to ciberbullying.* London: Corwin.

Hinduja, S., & Patchin, J. (2009). *Bullying beyond the schoolyard.* Thousand Oaks, CA: Sage.

INHOPE Foundation. (1999). *INHOPE.* Recuperado el 13 de 06 de 2015, de http://www.inhope.org/gns/who-we-are/at-a-glance.aspx

Insafe. (2000). *Safe Internet.* Obtenido de http://www.saferinternet.org/about

Insafe. (2013a). *Safer Internet.* Obtenido de http://www.saferinternet.org/about

Insafe. (2013b). *Safer Internet Day*. Obtenido de http://www. saferinternetday.org/web/guest/insafe-other

Insafe. (2015a). *Safer Internet Day.* Obtenido de http://www.saferinternetday .org/web/guest

Insafe. (2015b). *Safer Internet Day.* Obtenido de http://www.saferinternetday.

org/web/spain/home

INSAFE. (2015c). *Safer Internet Forum 2015.* Obtenido de http://www.saferinternet.org/sif

Insafe y Inhope. (2015). *Insafe - Inhope: working together for a better internet for children and young people.* Obtenido de http://www.saferinternet.org/c/document_library/get_file?uuid=0f285af4-8fff-489d-8da8-2298a8ed898d&groupId=10137

Instituto Nacional de Ciberseguridad de España. (2013). *INCIBE: Instituto Nacional de Ciberseguridad de España*. Recuperado el 25 de 08 de 2013, de https://www.incibe.es

Instituto Nacional de Estadística. (03 de 10 de 2016). *Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares.* Recuperado el 2017 de 01 de 11, de Equipamiento y uso de TIC en los hogares: http://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735976608

Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado. (2009). *INTEF*. Recuperado el 21 de 09 de 2014, de Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado: http://www.ite.educacion.es/es/intef

INTEF. (2013). *Riesgo del uso de la red para los menores.* Comparecencia en el Senado, Madrid.

Livingstone, S. H. (2011). *London School of Economics and Political Science.* Recuperado el 21 de 05 de 2014, de Risks and safety on the Internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online: http://eprints.lse.ac.uk/33731

Livingstone, S., & Helsper, H. (2007). *Gradations in digital inclusion: Children, young people and the digital divide.* London: SAGE Publications.

Livingstone, S., & Leslie, H. (2009). *EU Kids Online: Final Report.* EC Safer Internet Plus Programme Deliverable D6.5, LSE, London: EU Kids Online. Recuperado el 15 de 03 de 2013, de http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf

Livingstone, S., Ólafsson, K., O'neill, B., & Donoso, V. (2012). *Towards a better internet for children: findings and recommendations from EU Kids Online to inform the CEO coalition.* London. Obtenido de http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/EUKidsOnlinereportfortheCEOCoalition.pdf

Lucena Ferrero, R. (2003). Variables personales, familiares y escolares que influyen en el maltrato entre iguales (tesis doctoral). Universidad Complutense de Madrid, Madrid.

Mascheroni, G., & Cuman, A. (2014). *Net Children Go Mobile: Final report.* Milano: Educatt.

Minetur. (2002). *Red.es*. Recuperado el 08 de 08 de 2014, de www.red.es

Ministerio de ciencia y tecnología. (2003). *Programa de Actuaciones para el Desarrollo de la Sociedad de la Información en España.* Recuperado el 24 de 07 de 2015, de http://campus.usal.es/~derinfo/derinfo/Espana.es/espana_es.pdf

Ministerio de educación, cultura y deporte. (2015). *Infracciones del Derecho de utor.* Madrid. Recuperado el 2017 de 01 de 03, de Infracciones del derecho de autor: http://www.mecd.gob.es/cultura-mecd/dms/mecd/cultura-mecd/areas-cultura/propiedadintelectual/mc/guia-ompi/capitulos/InfraccionesDerecho Autor_C.pdf

Ministerio de Industria, Energía y Turismo y Ministerio de Hacienda y Administraciones Públicas. (2013). *Agenda Digital para España.* Obtenido de https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAAahUKEwjRmbv_2IXHAhUFPhQKHcC5BHM&url=http%3A%2F%2Fwww.agendadigital.gob.es%2Fagenda-digital%2Frecursos%2FRecursos%2F1.%2520Versi%25C3%25B3n%2520definitiva%2FAgenda_D

Ministerio de Industria, Energía y Turismo. (2013). *Agenda Digital para España*. Obtenido de http://www.agendadigital.gob.es/agenda-digital/Paginas/agenda-digital.aspx

Ministerio de Industria, Energía y turismo. (2013a). *Plan Avanza 2 - Informe de Seguimiento Madrid.* Madrid.

Ministerio de Industria, Energía y Turismo. (2013b). *Plan Avanza 2 - Informe de Seguimiento.* Madrid.

Ministerio de Industria, Energía y Turísmo. (2014). *Informe de seguimiento del Plan de Confianza en el Ámbito Digital.* Madrid. Obtenido de http://www.agendadigital.gob.es/planes-

actuaciones/Bibliotecaconfianza/2.%20Material%20complementario/ADPE-Situacion_Plan_5-3Q2014.pdf

Ministerio de Industria, Energía y Turismo y Ministerio de Hacienda y Administraciones Públicas. (2015). *Informe Anual de la Agenda Digital para España.* Madrid.

NICAM. (2013). *kijkwijzer*. Recuperado el 29 de 05 de 2016, de http://www.kijkwijzer.nl/nicam

NICAM y bbfc. (s.f.). *You Rate It*. Recuperado el 23 de 11 de 2015, de http://www.yourateit.eu/

Oficina de Seguridad del Internauta. (2013). *OSI*. Recuperado el 24 de 05 de 2016, de Oficina de Seguridad del Internauta: http://www.osi.es/es/quienes-somos

Pantallas Amigas. (2009). *PantallasAmigas*. Recuperado el 14 de 10 de 2013, de http://tecnoadiccion.es/acerca-de-tecnoadiccion-es/

Prensky, M. (2001). Digital Natives, Digital Immigrants. *On the Horizon*(9).

Princesa Lorelei. (2015). *Princesa Lorelei ProAna*. Obtenido de http://prinzessinloreleiwannabeana.blogspot.com.es/

Protégeles. (2005). *La prevención de la anorexia y la bulimia en internet.* Madrid. Recuperado el 07 de 07 de 2015, de https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCgQFjAA&url=http%3A%2F%2Fprotegeles.com%2Fdocs%2Festudio_anorexia.pdf&ei=PPqbVci-

NoGyU_L_gKAL&usg=AFQjCNHfZYp35yl7GNt8tQV0fSwUzm4Rbg&sig2=DxnR2TMMQVc_yMk_VskEjQ&bvm=bv.969

Protegeles. (2014). *Menores de Edad y Conectividad Móvil en España: Tablets y Smartphones.* Barcelona.

Protégeles y Cesicat. (2011). *Centro de internet segura*. Recuperado el 20 de 03 de 2015, de http://www.centrointernetsegura.es/definicion_del_proyecto.php

Protégeles y CESICAT. (2014). *Centro de Seguridad en Internet.* Barcelona. Obtenido de http://www.centrointernetsegura.es/descargas/dossier_2014_v1a1.pdf

Red.es. (08 de Agosto de 2015). *Monográfico ciberacoso escolar (Ciberbullying).* Recuperado el junio de 2015, de Chaval.es: http://www.chaval.es/chavales/content/descarga-de-contenidos-formacion

Red.es. (2015a). *Monográfico Acceso a contenidos inapropiados.* Obtenido de Chaval.es: http://formacion.chaval.es/component/jdownloads/send/11-contenidos-contenidos-inapropiados/54-mon-acceso

Red.es. (2015b). *Monográfico Comunidades peligrosas en línea*. Obtenido de Chaval.es: http://www.chaval.es/chavales/content/descarga-de-contenidos-formacion

Red.es. (2015c). *Monográfico Gestión de la privacidad e identidad digital.* Obtenido de Chaval.es: http://formacion.chaval.es/component/jdownloads/send/5-contenidos-gestion-privacidad/30-mon-gestion?option=com_jdownloads

Red.es. (2015d). *Monográfico Protección ante virus y fraudes.* Obtenido de Chaval.es: http://www.chaval.es/chavales/content/descarga-de-contenidos-formacion

Red.es. (2015e). *Monográfico Sexting.* Obtenido de Chaval.es: http://www.chaval.es/chavales/content/descarga-de-contenidos-formacion

Red.es. (2015f). *Monográfico Grooming.* Recuperado el 9 de Agosto de 2015, de Chaval.es: http://www.chaval.es/chavales/content/descarga-de-contenidos-formacion

Ruiz, J., Sánchez, J. y Gómez, M. (2013). Entornos personales de aprendizaje: estado de la situación de la Facultad de Ciencias de la Educación de la Universidad de Málaga. Píxel-Bit. Revista de Medio y Educación, 42, 171-181.

Safer Internet Day. (2015). *European Schoolnet*. Recuperado el 2016, de Safer Internet Day 2015. Luxemburgo.: http://www.saferInternetday.org/c/document_library/get_file?uuid=fbf1c3a3-2192-45c9-a787-28d1b06bfc5e&groupId=10136

Safer Internet Programme. (2010). *Benchmarking of parenta control tools for the online protection of children SIP-Bench II. Results of the 5th cycle.*

Safer Internet Programme. (2012). *Benchmarking of parental control tools for the online protection of children SIP-Bench II. Results of the 3rd cycle.*

Samsung Electronics. (2013). *Cinco razones por las que Galaxy Tab 3 Kids te ayuda a educar a tus hijos*. Recuperado el 07 de 12 de 2013, de http://www.samsung.com/es/article/galaxy-tab-3-kids-5-razones-por-las-que-te-ayuda-a-educar-a-tus-hijos/

Samsung Electronics. (2013). *Internet a Better Place For Children.* Implementation Report . Obtenido de http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=4432

Sanchez de León, J. (30 de 06 de 2015). *Reforma del Código Penal: nuevo régimen de los delitos contra la Propiedad Intelectual e Industrial*. Obtenido de Noticias Jurídicas: http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10300-reforma-del-codigo-penal:-nuevo-regimen-de-los-delitos-contra-la-propiedad-intelectual-e-industrial/

Secretaría de Estado de las Telecomunicaciones y para la sociedad de la información. (2005b). *Plan Avanza. Anexo I: Programa de Trabajo 2006. Medidas por áreas de actuación.* Madrid.

Secretaria de Estado de las Telecomunicaciones y para la Sociedad de la Información. (2014). *Plan de confianza en el ámbito digital 2013 - 2015. Agenda digital para España.* Madrid.

Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. (2005). *Plan 2006-2010 para el desarrollo de la Sociedad de la Información y de Convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas.* Madrid. Obtenido de http://www.agendadigital.gob.es/agenda-digital/planes-anteriores/Paginas/plan-avanza.aspx

Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. (2005a). *Plan Avanza. Anexo II. Medidas por áreas de actuación 2007-2010.* Madrid. Obtenido de http://www.agendadigital.gob.es/agenda-digital/planes-

anteriores/DescargasPlan%20Avanza/1.%20Plan%20Avanza/plan_avanza_AnexoII_Medidas20072010.pdf

Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. (2008). *Plan Avanza, Telecomunicaciones y Sector Audiovisual.* Madrid. Obtenido de http://www.agendadigital.gob.es/agenda-digital/planes-anteriores/DescargasPlan%20Avanza/2.%20Balance%20actuaciones%20(2008)/balance-actuacionsSetsi.pdf

Secretaría de estado de Telecomunicaciones y para la Sociedad de la Información. (2010a). *Plan Avanza 2. Anexos estrategia 2011 - 2015.* Madrid.

Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. (2010b). *Plan Avanza 2. Estrategia 2011 - 2015.* Madrid.

Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. (2013). *Plan Avanza*. Recuperado el 14 de 04 de 2016, de https://www.planavanza.es/Paginas/Inicio.aspx

Tomé Muguruza, B. (2001). El Plan de Acción INFO XXI. La Sociedad de la Información para todos. *Economía Industrial*(338), 19-23. Recuperado el 2015 de 07 de 24, de http://www.minetur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/338/02tome338.pdf

Trabazo, V. y Azor, F. (2011). *Gabinete de psicología*. Recuperado el 20 de 12 de 2014, de gabinetedepsicologia.com

UK Safer Internet Center. (2015). *Safer Internet Day*. Obtenido de http://www.saferinternetday.org/web/united-kingdom/home

Voz de América. (12 de 05 de 2015). *Redes sociales: "armas de reclutamiento" para terroristas*. Obtenido de VOA - Estados Unidos: https://www.voanoticias.com/a/redes-sociales-arma-para-reclutar-terroristas/2764274.html

W3C Group. (2013). *MIRACLE's common data model for age classification information and electronic labels.* Recuperado el 16 de 07 de 2015, de http://www.miracle-label.eu/wp-content/uploads/miracle-1-0/MIRACLE-Deliverable_D1-1_final.pdf

CAPÍTULO VII: ANEXOS

A continuación se exponen algunos documentos de interés utilizados para la presente investigación. El primer documento corresponde a la versión de la "Escala de competencia parental percibida" dirigida a los padres; el segundo de ellos, al mismo instrumento de evaluación en su versión destinada a los hijos. En ambos casos se encuentran, en un principio, el registro de los datos socio – demográficos, seguido de las instrucciones para cumplimentar la escala y finalmente la hoja de respuesta.

Finalmente, se presenta la carta enviada a las familias que participaron de la investigación.

1. CUESTIONARIO PRETEST HÁBITOS SEGUROS Y RESPONSABLES EN EL USO DE LAS TIC

Alumnos/as de 2º de la ESO

A continuación, te vamos a hacer algunas preguntas sobre ti y tus hábitos cuando te conectas a internet. Es importante que pongas atención e interés y, sobre todo, que respondas con sinceridad a todo lo que se te pregunta. No hay respuestas correctas ni incorrectas.

El cuestionario tiene asignado un identificador que nos permitirá emparejarlo con el cuestionario que se responderá al finalizar el estudio, siempre respetando la privacidad y el anonimato del mismo. Intenta no dejar ninguna cuestión sin contestar, son fáciles y tienes tiempo suficiente.

La forma de responder es sencilla, para cada cuestión debes marcar con una cruz la casilla que corresponda con tu respuesta, excepto en la primera pregunta que has de escribir tu edad.

Nº ID

1. ¿Cuántos años tienes? _____
2. Género: Hombre ☐ Mujer ☐
3. ¿Cuál es tu centro educativo?

   IES GARCÍA MORATO ☐

   IES ITURRALDE ☐

4. ¿A quién aceptarías como 'amigo' en tus redes sociales? Marca una sola respuesta
   Nota: las personas que no tienen redes sociales, también, han de responder la pregunta.

   ☐ A mis amigos

   ☐ A mis amigos y a amigos de mis amigos

   ☐ A mis amigos, amigos de mis amigos y a personas que conozco en internet

   ☐ A todo el mundo que me lo proponga

5. ¿Cuántas fotos, en las que apareces, tienes subidas a tus redes sociales?

	No tengo redes sociales	Ninguna	Entre 1 y 9	Entre 10 y 50	Entre 51 y 99	Entre 100 y 200	Más de 200
FOTOS	☐	☐	☐	☐	☐	☐	☐

6. Alguna de las fotos, en las que apareces, que tienes compartidas en tus redes sociales, ¿podría parecerles inadecuada a tus padres si la vieran?

	SI	NO	No tengo redes sociales
Fotos	☐	☐	☐

7. Alguno de los comentarios, que tienes en tus redes sociales, ¿podría parecerles inadecuado a tus padres si lo vieran?

	SI	NO	No tengo redes sociales
Comentarios	☐	☐	☐

8. ¿Consideras necesario configurar tú mismo/a la seguridad y privacidad de tus redes sociales? Nota: las personas que no utilizan redes sociales, también, han de responder la pregunta.

☐ SI
☐ NO
☐ No entiendo la pregunta

9. De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? Señala una respuesta para cada opción disponible.

	Sí	No
Con mis amigos	☐	☐
Con amigos de mis amigos	☐	☐
Con personas que he conocido en internet	☐	☐

10. ¿Qué tipo de información compartirías con personas que has conocido en internet? Señala una respuesta para cada opción disponible, marcando un cuadro por fila.

	Sí	No
E-mail	☐	☐
Nº de teléfono	☐	☐

11. De las siguientes ‘personas’, ¿con quienes utilizarías una webcam?
Señala una respuesta para cada opción disponible, marcando un cuadro por fila.

	Sí	No
Con mis amigos	☐	☐
Con amigos de mis amigos	☐	☐
Con personas que he conocido en internet	☐	☐

12. ¿Alguna vez te has burlado de una foto o comentario en una red social?

☐ SI
☐ NO
☐ No tengo redes sociales

13. ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu ordenador de casa? Si hay más de un ordenador en tu casa, responde en relación al ordenador que utilizas habitualmente.

	SI	NO	No tengo ordenador en casa
Ordenador en casa	☐	☐	☐

14. ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu Smartphone?

	SI	NO	No tengo Smartphone
Smartphone	☐	☐	☐

15. A continuación encontrarás una serie de afirmaciones que deberás contestar según tu grado de acuerdo o desacuerdo con cada una de las frases. Se ha empleado una escala de 5 puntos con las siguientes opciones de respuesta:

- Si estás totalmente en desacuerdo con la afirmación, marca ---------- 1
- Si estás bastante en desacuerdo con la afirmación, marca ---------- 2
- Si no estás ni de acuerdo ni desacuerdo con la afirmación, marca ------- 3
- Si estás bastante de acuerdo con la afirmación, marca ---------- 4
- Si estás totalmente de acuerdo con la afirmación, marca ---------- 5

	1	2	3	4	5
Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	☐	☐	☐	☐	☐
Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	☐	☐	☐	☐	☐
Sólo entro en páginas web recomendadas para mí edad	☐	☐	☐	☐	☐
Los chats públicos son páginas seguras donde nadie puede hacerme nada	☐	☐	☐	☐	☐
No pasa nada por descargar música o aplicaciones "pirateadas"	☐	☐	☐	☐	☐
Si conozco a alguien simpático/a jugando en red, le agregaría como 'amigo/a' en mi red social	☐	☐	☐	☐	☐
Si una página web me pide el número de teléfono, se lo doy	☐	☐	☐	☐	☐
Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	☐	☐	☐	☐	☐
Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	☐	☐	☐	☐	☐

16. ¿Han hablado contigo sobre los hábitos seguros y responsables cuando te conectas a internet?

☐ Si

☐ No

2. CUESTIONARIO POSTEST HÁBITOS SEGUROS Y RESPONSABLES EN EL USO DE LAS TIC

Alumnos/as de 2º de la ESO

A continuación, te vamos a hacer algunas preguntas sobre ti y tus hábitos cuando te conectas a internet. Es importante que pongas atención e interés y, sobre todo, que respondas con sinceridad a todo lo que se te pregunta. No hay respuestas correctas ni incorrectas.

El cuestionario tiene asignado un identificador que nos permitirá emparejarlo con el cuestionario realizado al comienzo del estudio, siempre respetando la privacidad y el anonimato del mismo. Intenta no dejar ninguna cuestión sin contestar, son fáciles y tienes tiempo suficiente.

La forma de responder es sencilla, para cada cuestión debes marcar con una cruz la casilla que corresponda con tu respuesta, excepto en la primera pregunta que has de escribir tu edad.

Nº ID

1. ¿Cuántos años tienes? _____
2. Género: Hombre ☐ Mujer ☐
3. ¿Cuál es tu centro educativo?

   IES GARCÍA MORATO ☐

   IES ITURRALDE ☐

4. ¿A quién aceptarías como 'amigo' en tus redes sociales? Marca una sola respuesta.
   Nota: las personas que no tienen redes sociales, también, han de responder la pregunta.

   ☐ A mis amigos

   ☐ A mis amigos y a amigos de mis amigos

   ☐ A mis amigos, amigos de mis amigos y a personas que conozco en internet

   ☐ A todo el mundo que me lo proponga

5. En el último mes, ¿has eliminado fotos o vídeos, en los que apareces, de tus redes sociales?

	No tengo redes sociales	Ninguna	Pocas	Algunas	Bastantes	Muchas
Fotos o vídeos	☐	☐	☐	☐	☐	☐

6. Alguna de las fotos, en las que apareces, que tienes compartidas en tus redes sociales, ¿podría parecerles inadecuada a tus padres si la vieran?

	SI	NO	No tengo redes sociales
Fotos	☐	☐	☐

7. Alguno de los comentarios, que tienes en tus redes sociales, ¿podría parecerles inadecuado a tus padres si lo vieran?

	SI	NO	No tengo redes sociales
Comentarios	☐	☐	☐

8. ¿Consideras necesario configurar tú mismo/a la seguridad y privacidad de tus redes sociales? Nota: las personas que no utilizan redes sociales, también, han de responder la pregunta.

☐ SI
☐ NO
☐ No entiendo la pregunta

9. En el último mes, ¿has revisado o modificado la configuración de seguridad y privacidad de tu red social? Nota: las personas que no utilizan redes sociales, también, han de responder la pregunta.

☐ SI
☐ NO
☐ No entiendo la pregunta

10. De las siguientes 'personas', ¿con quienes compartirías una foto o vídeo en el que aparezcas? Señala una respuesta para cada opción disponible.

	Sí	No
Con mis amigos	☐	☐
Con amigos de mis amigos	☐	☐
Con personas que he conocido en internet	☐	☐

11. ¿Qué tipo de información compartirías con personas que has conocido en internet?
Señala una respuesta para cada opción disponible, marcando un cuadro por fila.

	Sí	No
E-mail	☐	☐
Nº de teléfono	☐	☐

12. De las siguientes 'personas', ¿con quienes utilizarías una webcam?
Señala una respuesta para cada opción disponible, marcando un cuadro por fila.

	Sí	No
Con mis amigos	☐	☐
Con amigos de mis amigos	☐	☐
Con personas que he conocido en internet	☐	☐

13. ¿Alguna vez te has burlado de una foto o comentario en una red social?

☐ SI
☐ NO
☐ No tengo redes sociales

14. ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu ordenador de casa? Si hay más de un ordenador en tu casa, responde en relación al ordenador que utilizas habitualmente.

	SI	NO	No tengo ordenador en casa
Ordenador en casa	☐	☐	☐

15. ¿Tienes instalado software de protección, como por ejemplo un antivirus, en tu Smartphone?

	SI	NO	No tengo Smartphone
Smartphone	☐	☐	☐

16. A continuación encontrarás una serie de afirmaciones que deberás contestar según tu grado de acuerdo o desacuerdo con cada una de las frases. Se ha empleado una escala de 5 puntos con las siguientes opciones de respuesta:
    - Si estás totalmente en desacuerdo con la afirmación, marca ----------1
    - Si estás bastante en desacuerdo con la afirmación, marca----------2
    - Si no estás ni de acuerdo ni desacuerdo con la afirmación, marca-------3
    - Si estás bastante de acuerdo con la afirmación, marca ----------4
    - Si estás totalmente de acuerdo con la afirmación, marca ----------5

	1	2	3	4	5
Es imprescindible el uso de antivirus y otros programas de protección en tu ordenador, tablet y Smartphone	☐	☐	☐	☐	☐
Si conozco a una persona por internet que me da mucha confianza, le daría mi número de teléfono móvil	☐	☐	☐	☐	☐
Sólo entro en páginas web recomendadas para mí edad	☐	☐	☐	☐	☐
Los chats públicos son páginas seguras donde nadie puede hacerme nada	☐	☐	☐	☐	☐
No pasa nada por descargar música o aplicaciones “pirateadas”	☐	☐	☐	☐	☐
Si conozco a alguien simpático/a jugando en red, le agregaría como ‘amigo/a’ en mi red social	☐	☐	☐	☐	☐
Si una página web me pide el número de teléfono, se lo doy	☐	☐	☐	☐	☐
Si conozco a alguien por internet que me cae bien y me da confianza, quedaría para conocernos en persona	☐	☐	☐	☐	☐
Insultar, o vacilar, a un/a compañero/a o amigo/a en una red social es menos humillante que decírselo en persona	☐	☐	☐	☐	☐

17. ¿Han hablado contigo sobre los hábitos seguros y responsables cuando te conectas a internet?

    ☐ Si

    ☐ No